European Technology Risk Assessment

By Glen Birkbeck
January 2026

Contents

European Technology Risk Assessment

This work was independently authored by Glen Birkbeck. Artificial intelligence tools were used for research assistance, fact checking, and drafting support, but all analysis, structure, judgment, and final content reflect the author's own expertise and responsibility.

This is revision 2 of the **European Technology Risk Assessment**, incorporating structural updates for improved flow, including a dedicated chapter on AI and emerging risks, another dedicated chapter on internet core (BGP, DNS, PKI), while building on prior versions.

This publication is for informational purposes only and does not constitute legal, financial, or professional advice.

Chapter 1: Executive Summary

In an era of intensifying great-power rivalry, this executive summary outlines the critical technology risks facing European businesses amid conflicts in Ukraine, tensions over Taiwan, and potential U.S. policy shifts. It highlights key geopolitical drivers, the scope of the assessment, and strategic recommendations to build resilience and digital sovereignty. Executives can use this overview to prioritise actions like supply chain diversification and scenario planning, with deeper details available in subsequent chapters.

This technology risk assessment is primarily designed to equip European and UK businesses with a clear-eyed understanding of emerging and evolving technology-related risks driven by today's volatile geopolitical environment. However, its insights and frameworks are also highly relevant and applicable to businesses in the Canada, and other countries or alliances facing similar geopolitical and technological challenges. As great-power competition intensifies, Europe finds itself at the intersection of multiple overlapping threat vectors - from kinetic conflict on its eastern flank to digital and economic coercion emanating from both Moscow and Beijing, compounded by potential instability in transatlantic relations due to shifting U.S. policies.

Key Drivers of Risk

A common misconception is that the internet was designed to survive a nuclear exchange, rooted in ARPANET's packet-switching for redundancy. While that core resilience held in early days, today's layered architecture—dominated by U.S. hyperscalers, vulnerable supply chains, and concentrated infrastructure—exposes it to targeted geopolitical threats like cable sabotage or export controls. This assessment reveals how these evolutions demand renewed sovereignty strategies for European businesses.

The assessment identifies three primary geopolitical flashpoints that are reshaping the technology risk landscape for European enterprises:

- **Russia's Sustained Aggression Against Ukraine**: Now in its fourth year, this conflict has escalated from territorial disputes to a broader campaign of infrastructure attrition. Russian forces have systematically targeted Ukrainian energy, transportation, and civilian systems, with spillover effects threatening EU neighbors. Notable incidents include drone strikes on gas stations near Romanian borders in August 2025 and unexplained subsea cable disruptions in the Baltic Sea, raising alarms about covert sabotage. These actions demonstrate how hybrid warfare, combining kinetic attacks, cyber operations by groups like APT28 (Fancy Bear), and energy coercion, can isolate regions, disrupt supply chains, and undermine economic stability. For European businesses, this translates to heightened vulnerabilities in energy grids, logistics networks, and critical connectivity, especially in Central and Eastern Europe.
- **China's Military Posturing Toward Taiwan**: With over 90% of the world's advanced logic chips produced in Taiwan by TSMC, any escalation in cross strait tensions could trigger immediate global shortages. A blockade, missile campaign, or invasion would halt semiconductor deliveries within days, crippling European industries reliant on just in time manufacturing for automotive, industrial automation, and telecommunications. Beyond chips, China's dominance in rare earths, 5G equipment, and AI surveillance technologies creates dependencies that complicate EU sanctions and supply chain audits. State backed acquisitions of European fabs and cloud stakes further risk embedded backdoors or forced data localization, challenging Europe's digital sovereignty ambitions.
- **Potential U.S. Policy Volatility Under Frameworks Like Project 2025**: Domestic shifts in the U.S., such as changes to federal labor protections, export controls, and intelligence sharing norms, are eroding transatlantic trust. European firms depending on American cloud providers (AWS, Azure), cybersecurity vendors, or software ecosystems may face compliance conflicts with GDPR, reduced interoperability, or politicized access to advanced technologies. This uncertainty amplifies

risks for businesses in sectors like AI development and data-intensive operations, where U.S. based control planes and model training data reside outside EU jurisdiction.

These dynamics collectively challenge Europe's pursuit of **digital sovereignty**, **supply chain resilience**, and **business continuity**. The convergence of cyber, physical, regulatory, and market access risks demands proactive mitigation, not just reactive compliance.

Scope and Structure of the Assessment

This document provides a comprehensive, actionable framework for European enterprises to navigate these threats. It is structured as follows. Each chapter includes a conclusion recapping key insights for quick reference.

- **Chapter 2: Geopolitical Context and Strategic Threat Landscape** delves into the interlocking flashpoints of U.S. policy shifts, Russia's hybrid tactics, and China's strategic ambitions, illustrating their direct implications for European technology dependencies and digital sovereignty.
- **Chapter 3: Critical Technology Domains at Risk** examines core domains—telecommunications, energy systems, cloud infrastructure, and semiconductors—highlighting vulnerabilities like undersea cable exposure, grid synchronization with conflict zones, data localization conflicts, and Asian manufacturing reliance.
- **Chapter 4: AI, Dual-Use & Emerging Risks** delves into artificial intelligence, surveillance technologies, and emerging threats like quantum computing and edge AI, exploring dependencies on U.S. hardware/models/cloud, ethical challenges, and pathways to sovereignty (e.g., Mistral AI, EU AI Act). It builds on Ch3 domains with strategies for dual-use compliance and resilience.
- **Chapter 5: Internet Core Sovereignty and Digital Resilience** provides a deep dive into foundational internet protocols (BGP for routing, DNS for resolution, TLS/PKI for security) and sovereignty strategies amid U.S. rupture risks. It builds on Ch3/Ch4's infrastructure and AI vulnerabilities with phased implementation roadmaps; detailed browser/comms/payment tools in Appendix E.
- **Chapter 6: Threat Vectors and Attack Scenarios** outlines realistic attack methods, from state sponsored cyber operations (e.g., Industroyer2 variants targeting grids) to disinformation campaigns manipulating corporate decisions, with plausible scenarios like "GridLock Winter" or "Chip Panic" to illustrate cascading impacts.
- **Chapter 7: Regulatory and Compliance Landscape** reviews key EU instruments such as the Cyber Resilience Act (CRA), NIS2 Directive, and GDPR, noting gaps where compliance does not equate to resilience during crises, and addressing export controls and due diligence under frameworks like the Dual Use Regulation.
- **Chapter 8: Risk Mitigation Framework** offers a multi tiered approach with pillars including supply chain diversification (e.g., onshoring via EU Chips Act initiatives), cyber hygiene with Zero Trust architectures, continuity planning for redundant connectivity and energy autonomy, scenario based exercises, and rigorous vendor risk management.
- **Chapter 9: Public/Private Collaboration and Policy Recommendations** emphasizes the need for coordinated action, proposing roles for ENISA, EEAS, and national CERTs, industry coalitions like ISACs, and policy incentives for sovereign infrastructure investments.
- **Appendices** include a glossary of terms, maps of high-risk corridors, a self assessment checklist, and key resources for ongoing monitoring.

Strategic Recommendations and Goals

The assessment empowers European businesses to:

- Conduct thorough vulnerability assessments across critical domains, identifying dependencies on non EU suppliers and infrastructure.
- Develop layered mitigation strategies, from diversifying supply chains to implementing advanced cybersecurity and contingency planning.
- Engage with evolving EU regulations while anticipating geopolitical shocks through scenario planning and public/private partnerships.
- Position themselves as resilient actors in a contested technological landscape, balancing competitiveness with sovereignty.
- Audit cloud vendor share and negotiate sanctions exit clauses to reduce concentration risks [Japan Times].
- Perform data residency audits and adopt end to end encryption to counter U.S. law enforcement overreach [Atlantic Council].
- Allocate budgets for transitioning to EU alternatives and joining sector wide resilience alliances [Politico EU].
- Implement Chapter 4's phased sovereignty strategies, such as RPKI for secure routing, EU Root CA for encryption trust, and EPI/wero for payment autonomy, to counter transatlantic disruptions.

Ultimately, this document serves as a strategic guide for executives, CISOs, supply chain leaders, and compliance officers. By addressing technology risks through a geopolitical lens, it aims not only to safeguard operations but to enable European enterprises to thrive amid uncertainty, fostering innovation and collaboration in an era where technology is both a vulnerability and a source of strength.

Chapter 2: Geopolitical Context and Strategic Threat Landscape

This chapter explores the geopolitical forces reshaping technology risks for European and UK businesses, focusing on Russia's war in Ukraine, China's ambitions towards Taiwan, and uncertainties in U.S. policy. It explains how these crises intersect to challenge digital sovereignty and supply chains, offering insights for executives to anticipate and mitigate broader impacts. Detailed analysis follows on transatlantic volatility, Russian hybrid tactics, and Chinese strategic pressures, with implications for business continuity.

Europe operates today in an era of compounded geopolitical instability. No longer can technology strategy be decoupled from the realities of war, great power rivalry, or transatlantic political volatility. Three interlocking flashpoints define the current threat environment, each amplifying the others in a cycle of escalating risk.

2.1 U.S. Policy Volatility and Transatlantic Uncertainty

The potential implementation of governance frameworks such as **Project 2025** introduces significant uncertainty into U.S. - EU technological alignment. While often discussed in domestic political terms, elements of this agenda carry direct implications for European businesses reliant on American partners. Project 2025, a blueprint for conservative governance, proposes sweeping changes to federal institutions, including deregulation of labour protections, which could destabilise U.S. based tech vendors and cloud providers. For instance, weakening OSHA standards might lead to higher turnover or strikes in data centres, disrupting service levels for European clients.

For example, recent directives from the U.S. Office of Personnel Management (OPM) now permit federal employees to openly promote religious beliefs in the workplace, display religious materials, and engage in collective prayer. Though seemingly internal, such shifts signal a broader reorientation of U.S. institutional norms, one that may extend to regulatory agencies overseeing export controls, cybersecurity standards, and intelligence sharing protocols. This cultural pivot could foster an environment where ideological biases influence technical decisions, such as prioritizing certain vendors over others based on political affiliations.

More concretely, a Project 2025 influenced administration could:

- Reconfigure **export control regimes** (e.g., tightening or politicizing access to advanced semiconductors, AI models, or cloud infrastructure), potentially delaying EU access to cutting edge GPUs needed for AI training;
- Reduce interoperability with EU data protection and digital sovereignty frameworks (e.g., weakening Privacy Shield type agreements), forcing European firms to renegotiate data flows or face costly alternatives;
- Prioritize ideological alignment over technical cooperation in **intelligence and cyber defence partnerships**, potentially fragmenting joint threat response capabilities and leaving gaps in shared intelligence on Russian or Chinese cyber threats.

For European firms using U.S. based cloud providers like AWS or Azure, cybersecurity vendors such as CrowdStrike, or software ecosystems reliant on Microsoft tools, these shifts represent not just compliance risks, but operational vulnerabilities if transatlantic trust erodes. Recent events underscore this volatility: in early January 2026, U.S. forces conducted a direct military operation in Venezuela, capturing President Nicolás Maduro and his wife in Caracas, marking a bold escalation from sanctions to intervention that could strain global alliances and complicate intelligence sharing norms. Similarly, the U.S. has intensified efforts to acquire Greenland, declaring it a "national security priority" and prompting EU protests and threats of tariffs, highlighting expansionist ambitions that might prioritize U.S. interests over multilateral tech cooperation.

2.2 Russia's Hybrid Warfare Against Europe's Technological Foundations

Russia's full scale invasion of Ukraine, now entering its fourth year, has evolved into a sustained campaign of **infrastructure attrition** with direct spillover risks for the EU. According to ACLED's August 2025 Conflict Monitor, Russian forces continue systematic strikes on civilian infrastructure, including energy, health, and transportation systems, with over **1,437 political violence events recorded in one week alone**. This relentless pressure has transformed the conflict from a regional dispute into a laboratory for hybrid warfare, testing tactics that blend conventional military action with cyber, economic, and informational elements.

Critically, Russia's targeting has expanded beyond Ukrainian territory, creating a ripple effect that endangers EU stability:

- On **6 August 2025**, Russian drones struck the **Orlivka gas transportation and compression station** in Odesa Oblast, located directly on the Romanian border. The attack triggered Romania's F-16 scramble and endangered the **Isaccea-Orlivka-Vulcănești-Chișinău high-voltage power line**, a key project designed to reduce Moldova's dependence on Russian-controlled Transnistria. This incident not only disrupted gas flows but also highlighted the fragility of interconnectors that EU policymakers had touted as safeguards.
- These strikes are not isolated. ACLED notes a rebound in energy infrastructure attacks, from ~30 in April 2025 to **~60 in both June and July**, despite a nominal March moratorium. Such patterns suggest Russia is calibrating its aggression to maximize economic pain without triggering full NATO escalation, using drones and missiles to probe defences and exhaust resources.

Beyond kinetic strikes, Russia employs **hybrid tactics** that threaten European technology resilience on multiple fronts:

- **Undersea cable sabotage**: Multiple incidents in the Baltic Sea since 2022, including cuts near Gotland in 2023 and 2024, have raised NATO alarms. Submarine communications cables linking Finland, Sweden, Germany, and the Baltics remain vulnerable to covert disruption, potentially isolating Nordic countries from global internet and financial networks. Repair times can exceed weeks, during which data routing must detour through less secure paths.
- **Cyber operations**: Persistent APT28 (Fancy Bear) and Sandworm campaigns target energy grids, logistics, and government IT systems across Central and Eastern Europe. For example, Sandworm's 2024 intrusions into Polish rail systems disrupted freight routes, while APT28 has been linked to phishing campaigns against EU defence contractors, stealing blueprints for dual use technologies.
- **Energy coercion**: By degrading Ukraine's ability to store or transit gas, Russia indirectly pressures EU winter preparedness, especially in Southeastern Europe. With EU gas storage at 85% capacity as of late 2025, any further disruptions could force rationing, impacting data centres that rely on stable power for cooling and operations.

The message is clear: critical infrastructure is now a frontline domain in great power conflict. Russian tactics demonstrate how a single drone strike or cyber exploit can cascade into regional crises, from blackouts in Bucharest to stock market volatility in Frankfurt.

2.3 China's Strategic Advance and the Taiwan Flashpoint

While less immediately kinetic than the Ukraine war, China's long term technological ambitions pose equally severe systemic risks to European businesses. Beijing's pursuit of **semiconductor self sufficiency**, dominance in rare earths processing, and control over global ICT standards directly challenges EU supply chain security. China's "Made in China 2025" initiative, now evolving into more aggressive industrial policies, aims to capture 70% of global semiconductor production by 2030, leveraging subsidies and espionage to close the gap with Taiwan and South Korea.

The most acute near term risk stems from **cross-strait tensions**, where any escalation could unleash immediate chaos:

- Over **90% of the world's most advanced logic chips** are manufactured in Taiwan by TSMC. Any Chinese blockade, amphibious assault, or missile campaign would trigger immediate, cascading shortages in automotive, industrial, medical, and telecom sectors across Europe. For instance, Volkswagen's production lines could halt within days, as modern vehicles rely on TSMC's chips for infotainment and autonomous features.
- Even short of war scenarios (such as export restrictions, port closures, or insurance market collapse) could halt chip deliveries within weeks. In 2025, Taiwan's semiconductor exports reached $120 billion, with Europe accounting for 15%, underscoring the continent's exposure.

Simultaneously, China leverages **dual use technology exports** (e.g., surveillance AI, quantum sensors, 5G equipment) to gain influence in third countries, creating indirect dependencies that complicate EU sanctions enforcement and supply chain audits. Huawei's 5G infrastructure in Southern Europe, for example, provides backhaul for critical services but embeds proprietary code that could be remotely updated or exploited. Chinese state backed entities also increasingly acquire stakes in European semiconductor fabs, battery plants, and cloud infrastructure, raising concerns about embedded backdoors or forced data localization. Notable acquisitions include SMIC's partnerships with German firms and Alibaba's investments in Dutch data centres, potentially allowing Beijing to influence EU data flows under the guise of commercial deals.

2.4 Implications for European Digital Sovereignty and Supply Chain Resilience

Together, these pressures expose a fundamental paradox: Europe seeks **digital sovereignty**, yet remains deeply enmeshed in transatlantic and transpacific technology ecosystems vulnerable to geopolitical rupture. This entanglement is not accidental but the result of decades of globalization that prioritized efficiency over security, leaving Europe reliant on foreign suppliers for core technologies.

Key implications include:

- **Overreliance on non EU cloud and AI infrastructure**, subject to foreign legal jurisdiction and policy whims; for example, U.S. CLOUD Act demands could compel providers to hand over European data, conflicting with GDPR and exposing trade secrets (see Chapter 4 for internet core sovereignty strategies like EU Root CA and DNS4EU).
- **Concentrated supply chains** for chips, batteries, and optical networking gear, with single points of failure in Taiwan, South Korea, or U.S. fabs; Europe's semiconductor production stands at just 10% of global output, compared to 60% in Asia.
- **Insufficient redundancy** in critical connectivity (e.g., limited alternative routes for subsea cables or energy interconnectors), where the Baltic Sea's 30+ cables have only 2-3 landing points per country, making sabotage devastating.
- **Regulatory fragmentation**, where NIS2, CRA, and GDPR compliance does not equate to operational resilience during active conflict or embargo; many firms pass audits but lack contingency plans for geopolitical shocks (detailed in Chapter 4's Digital Sovereignty Act proposals).

In this landscape, risk mitigation cannot be siloed within IT or procurement departments. It demands **enterprise wide scenario planning**, **sovereign alternatives**, and **public/private coordination**, themes explored in subsequent chapters. By confronting these realities head on, European businesses can transform vulnerabilities into opportunities, driving innovation in secure, resilient technologies that strengthen the continent's position in a multipolar world.

2.5 Conclusions

The geopolitical flashpoints outlined—U.S. volatility, Russian hybrid tactics, and Chinese strategic advances—directly threaten the critical technology domains detailed in Chapter 3. From transatlantic

export controls to Baltic cable vulnerabilities, these forces underscore the urgency of building digital sovereignty. European enterprises must integrate geopolitical awareness into strategy to navigate this multipolar world effectively.

Chapter 3: Critical Technology Domains at Risk

This chapter identifies key technology areas vulnerable to geopolitical disruptions, such as telecommunications, energy systems, cloud infrastructure, and semiconductors, with a focus on risks like undersea cable sabotage and supply chain dependencies. It provides executives with an overview of high-impact domains and initial metrics for assessment, before delving into detailed vulnerabilities and mitigation steps. Understanding these domains helps prioritise investments in resilience for European and allied businesses; AI and emerging risks are covered in Chapter 4.

Scenario Context (Q3 2026)

Europe's digital economy faces heightened risk due to the U.S. 6-month NATO exit timeline, tech sanctions on EU critical infrastructure, reciprocal EU restrictions, and rising sabotage risks (undersea cable tampering, DNS hijacking). This chapter assesses how these geopolitical shocks threaten interconnected technology domains and outlines actionable mitigation strategies.

Europe's digital economy rests on interconnected technological systems that are increasingly exposed to geopolitical shocks. This chapter examines core critical domains where disruption—whether through sabotage, supply chain failure, regulatory divergence, or cyberattack—could cascade across sectors and borders; AI and emerging tech in Chapter 4.

3.1 Telecommunications & Connectivity

Undersea Cable Vulnerability (Baltic/North Sea Routes)

Over 95% of international data traffic between Europe and the rest of the world flows through undersea fibre-optic cables. The Baltic Sea alone hosts more than **30 active subsea cables**, linking Finland, Sweden, Estonia, Latvia, Germany, and Denmark. These routes are now high value targets:

- In 2023 and 2024, unexplained cable cuts near Gotland and the Åland Islands raised NATO concerns about covert Russian naval activity.
- Repair vessels require weeks to deploy, and redundancy is limited, especially for countries like Estonia or Latvia, which rely on just 2 to 3 major cable landings.
- A coordinated attack on multiple cables during winter could isolate the Nordic - Baltic region from global cloud services, financial networks, and emergency communications.

5G/6G Dependencies on Non EU Vendors

Despite EU efforts to diversify, European 5G rollout remains heavily dependent on **Ericsson (Sweden)** and **Nokia (Finland)**, both capable but lacking full stack semiconductor sovereignty. Meanwhile, Huawei and ZTE remain present in legacy infrastructure across Southern and Eastern Europe, creating long term maintenance and security liabilities.

As 6G standardization accelerates (targeting 2030 deployment), Europe risks falling behind in core IP development, especially in AI, native radio access networks and terahertz spectrum management—areas where China and the U.S. are investing billions.

> **Key Risk**: Single point failures in physical connectivity + strategic lag in next generation telecom innovation.

Risk Metrics:

- Non EU cable redundancy share <40% (red flag); target ≥70%
- 5G/6G vendor reliance on non EU providers >60% (red flag); target <30%

Mitigation & Preparedness:

- Activate satellite backup projects (e.g., NATO's HEIST)

- Fund EU led undersea cable projects (Atlantic Link 2)
- Accelerate EU semiconductor and telecom R&D

3.2 Energy & Industrial Control Systems (ICS/OT)

Grid Security Amid Russian Strikes on Ukrainian Infrastructure

Russia's campaign against Ukraine's power grid has demonstrated how kinetic attacks can disable SCADA and ICS systems at scale. With shared grid interconnectors (e.g., ENTSO-E synchronization with Ukraine and Moldova since 2022), European operators face spillover risks:

- Cyberattacks like **Industroyer2** have already targeted Ukrainian substations; similar malware could be repurposed against Polish, Romanian, or Slovak grids.
- Many EU distribution networks still run on outdated OT protocols (Modbus, DNP3) with minimal segmentation from corporate IT networks.

Risks to Gas Interconnectors and LNG Terminals

While EU gas storage levels are high, physical infrastructure remains vulnerable:

- Key interconnectors (e.g., Poland – Lithuania GIPL, Romania – Hungary BRUA) pass near conflict prone regions.
- LNG terminals in Germany (Wilhelmshaven), Poland (Świnoujście), and Croatia (Krk) are potential targets for drone or sabotage operations, especially if Russia seeks to amplify energy panic ahead of winter.

  Key Risk: Convergence of cyber physical threats to energy delivery, with cascading impacts on manufacturing, data centres, and public safety.

Risk Metrics:

- ICS/OT vendor reliance on non EU providers >60% (red flag); target <30%
- Grid outage duration >6 hours (red flag); target <2 hours

Mitigation & Preparedness:

- Segment OT networks from IT
- Accelerate firmware patching (<6 hours)
- Stockpile EU-made ICS hardware

3.3 Cloud, Data Centres & Digital Infrastructure

Cloud, Data Centres & Digital Infrastructure Overview

U.S. hyperscalers (AWS, Azure, Google Cloud) dominate >60% of the global market, with control planes outside EU jurisdiction, creating CLOUD Act-GDPR conflicts and concentration risks (e.g., 2023 Amsterdam Trade Bank collapse due to U.S. sanctions) [Japan Times], [Politico EU]. Physical resilience in Eastern Europe is vulnerable to hybrid threats, while 70% DNS queries route via U.S. providers (Akamai, Cloudflare), risking hijacking/blocking [Akamai]. Server (80% U.S. hardware like Intel/AMD), integration (60% U.S. tools like MuleSoft), payments (45% U.S. via Stripe/PayPal/CHIPS), cybersecurity (75% U.S. supply chains), and devices (65% U.S.-made like Apple) amplify dependencies, with cascading failures possible (e.g., cloud outage halting payments) [European Parliament], [NIST], [U.S. Department of Homeland Security].

- **Risk Metrics**: U.S. cloud share >60% (red flag, target <30%); non-EU DNS routing <50% (target ≥80%); U.S. payment share <50% (target ≥80%); U.S. device reliance >60% (target <30%).
- For detailed mitigations like BGP reconfiguration, EU DNS resolvers (DNS4EU), TLS/PKI sovereignty (EU Root CA, DANE), payment rails (EPI/wero), and browser strategies (Firefox

investment), see Chapter 4. Contract audits and EU alternatives (e.g., OVHcloud, SEPA, Adyen) remain essential starting points.

Summary Table: Critical Domains, Metrics, and Mitigation Actions

Domain	Key Risk Metric (Red Flag)	Target	Mitigation Action
Telecom	Non EU cable redundancy <40%	≥70%	Satellite backup, new cables
Energy/ICS	ICS vendor reliance >60%	<30%	Segment OT, patch firmware
Cloud/Digital Infra	U.S. cloud/DNS reliance >60%/<50%	<30%/≥80%	See Ch5 for sovereignty plans; audit vendors
Semiconductors	Asian manufacturing >60%	<40%	EU Chips Act onshoring
AI/Dual-Use	Export non-compliance risks	Full due diligence	See Ch4 for AI details; Regulation 2021/821 adherence

3.4 Semiconductors & Hardware Supply Chains

Reliance on Asian Manufacturing (TSMC, Samsung)

Europe's semiconductor production stands at just 10% of global output, compared to 60% in Asia. TSMC alone produces over 90% of advanced logic chips (5nm and below), with fabs concentrated in Taiwan. A cross strait escalation could halt deliveries within days, crippling industries from automotive (infotainment systems) to healthcare (diagnostic equipment).

- TSMC's Arizona and Japan fabs won't reach full capacity before 2026–2027, and even then, will prioritize U.S. defence and consumer electronics.
- A Taiwan contingency could halt advanced chip shipments within **10–14 days**, idling European production lines.

EU Chips Act: Progress vs. Real-World Bottlenecks

The €43 billion EU Chips Act aims to double Europe's market share to 20% by 2030. Promising investments include:

- Intel's €30B "Silicon Junction" in Germany (2027 target)
- STMicroelectronics/GlobalFoundries joint venture in France
- Bosch's 300mm fab in Dresden

Yet bottlenecks persist:

- Shortage of skilled process engineers
- Limited EU based equipment makers (ASML dominates lithography but relies on U.S. and Japanese components)
- Slow permitting for cleanroom construction

  Key Risk: Strategic ambition outpaces execution timeline, leaving Europe exposed during the 2025–2028 window of maximum vulnerability.

- **Key Vulnerabilities**: Single source dependencies for GPUs, memory chips, and sensors; long lead times (6-12 months) for custom ASICs; exposure to export controls from China or the U.S.

Risks from Rare Earths and Dual Use Materials

China dominates 60% of rare earth mining and processing, essential for magnets in EVs, wind turbines, and electronics. U.S. or EU sanctions could trigger retaliatory restrictions, as seen in 2023 when China limited gallium exports.

- **Mitigation Strategies**: Diversify sourcing (e.g., U.S. Mountain Pass mine, Australian Lynas Corp.); invest in recycling technologies; stockpile critical materials under EU Critical Raw Materials Act.

  Key Risk: Fragile supply chains for foundational components, where geopolitical tensions can cause immediate, cascading failures across multiple sectors.

3.5 Conclusions

The core domains examined—telecommunications, energy, cloud, and semiconductors—form the backbone of Europe's digital economy, vulnerable to the geopolitical shocks in Chapter 2. These foundational risks set the stage for emerging AI risks in Chapter 4, where dependencies on these domains amplify threats. By prioritizing resilience in these areas, businesses can mitigate cascading failures and prepare for the sovereignty strategies in Chapter 5.

Chapter 4: AI, Dual-Use & Emerging Risks

This chapter focuses on artificial intelligence (AI), dual-use technologies, and emerging risks like quantum computing and edge deployment, building on the foundational domains in Chapter 3 (e.g., AI's reliance on semiconductors and cloud infrastructure). It explores dependencies, ethical challenges, and pathways to sovereignty, providing executives with strategies to mitigate geopolitical vulnerabilities in these high-impact areas. Detailed risks and mitigations tie to broader threats in Chapter 6 and sovereignty measures in Chapter 5.

4.1 AI, Surveillance & Dual Use Technologies

Export Control Compliance (EU Dual Use Regulation)

The EU's updated Dual Use Regulation (Regulation (EU) 2021/821) now covers **cyber intrusion tools, AI enabled surveillance systems, and quantum sensors**. Companies developing or integrating such technologies must conduct rigorous end user due diligence, especially when selling to entities in third countries with weak human rights records.

Non compliance risks include:

- Fines up to 10% of global turnover
- Reputational damage from inadvertent complicity in repression
- Loss of access to U.S. or allied technology ecosystems
- **Challenges**: Compliance with Regulation (EU) 2021/821 requires rigorous due diligence; failures can lead to fines or bans.
- **Ethical Risks**: AI integration in critical sectors raises concerns over bias, privacy, and misuse, especially with Chinese or Russian technology embedded in supply chains.

  Key Risk: Speed of AI adoption outpaces governance, creating new attack surfaces in previously "dumb" infrastructure.

AI Dependencies and Risks The rapid acceleration of Artificial Intelligence (AI) adoption, driven by Large Language Models (LLMs), introduces a distinct and critical layer of dependency in the European digital ecosystem. While traditional internet services rely on foundational protocols, AI systems introduce new choke points: access to advanced computational hardware, the export-controlled "intelligence" of AI models, and the data-intensive infrastructure that powers them. In a scenario where Europe is strategically severed from the United States, this dependency evolves from a mere service disruption into a profound strategic vulnerability, stifling innovation, economic security, and technological sovereignty.

European reliance on U.S. AI infrastructure is a tripartite challenge that spans hardware, software, and connectivity.

- **The Hardware Core: Advanced Chips Under Export Control**
  The sophisticated semiconductors required to train and run frontier AI models are overwhelmingly produced by U.S. companies (e.g., NVIDIA, AMD) and their supply chain partners. The U.S. government has enacted stringent export controls, designating these chips and the equipment to manufacture them as critical to national security. These controls create a licensing regime where shipments to "close U.S. allies" are favoured, while transfers to other nations, even for commercial use, are subject to strict processing power quotas. In a deteriorating transatlantic relationship, Europe's access to the next generation of these computational building blocks could be throttled or denied, directly capping its ability to advance its own AI capabilities independently.
- **The "Crown Jewels": Controlled AI Model Weights**
  The U.S. has taken the unprecedented step of classifying the model weights of the most advanced

AI systems as controlled technology, on par with advanced weaponry. Model weights are the proprietary, computationally-intensive essence of an AI model; they define its capabilities and cannot be easily replicated. Exports of these "frontier" weights are presumptively denied to any nation not considered a close ally. For European companies and researchers, this means the core intelligence of leading AI systems could be placed out of reach, forcing them to rebuild capabilities from a less advanced baseline and creating a potentially insurmountable innovation gap.

- **Cloud Infrastructure and Network Asymmetry**
  AI services are predominantly delivered via the cloud, a market where U.S. hyperscalers—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud—command approximately **63% of the global market**. These providers operate massive, globally-distributed data centres optimised for AI workloads. A disconnection from the U.S. would not only cut Europe off from these specific data centres but also from the proprietary global network backbones these companies have built to ensure low-latency, high-bandwidth connectivity for AI services. This dependency creates a critical asymmetry: while European providers like OVHcloud are growing, they lack the scale and integrated global infrastructure to seamlessly replace the capacity and performance of the U.S. giants.

In an isolation event, the technical dependencies translate into immediate and severe strategic consequences.

1. **Economic and Innovation Stagnation**: European businesses, from startups to multinationals, rely on U.S. cloud platforms to run data analytics, customer service automation, and R&D. A cutoff would freeze these operations. More critically, the inability to access leading-edge model weights and sufficient advanced computing hardware would cause Europe's AI sector to fall permanently behind, losing competitiveness in a domain central to future economic growth.
2. **Data Sovereignty and Security Inversion**: The concentration of European data in U.S.-controlled cloud regions, driven by performance and cost, becomes a liability. In a conflict, data governed by EU regulations (**GDPR**) could become inaccessible or subject to U.S. jurisdiction. Furthermore, the cybersecurity benefits of AI—real-time threat detection, automated response—which are increasingly vital for national infrastructure, would be degraded if the AI models and platforms powering them are unavailable.
3. **Geopolitical Leverage and Compliance Burden**: U.S. export controls are not static. They are a tool of statecraft. Europe's AI development would become subject to the shifting priorities of U.S. foreign policy, with compliance creating a massive administrative burden for companies. The U.S. AI Action Plan explicitly links technological leadership with national security, framing telecommunications and AI infrastructure as critical and requiring them to be "free from foreign adversary" influence—a definition that could become fluid in a crisis.

This ties to Chapter 6's "Taiwan Blockade" scenario (chip shortages) and Chapter 5's cloud sovereignty (63% U.S. market reliance). For Canada: Leverage CSE for AI security; UK: AI Safety Institute for model audits.

Strategic Pillar	Key Actions	Reference in Scenario
Sovereign Compute & Chip Diplomacy	Accelerate EU initiatives like the European Chips Act. Forge strategic partnerships for secure hardware supply. Develop "data-centre-validated end user" status within U.S. export frameworks.	Ensures access to the physical hardware needed to train and run sovereign AI models, independent of discretionary U.S. licences.

Strategic Pillar	Key Actions	Reference in Scenario
Invest in Sovereign AI Foundations	Massively fund open-source, Europe-based foundation model development (e.g., akin to Aleph Alpha). Create shared, secure research data spaces.	Builds indigenous "model weight" intellectual property not subject to U.S. export controls, creating a base for innovation.
Scale Sovereign Cloud & "Gaia-X"	Provide decisive market incentives to scale European cloud providers. Enforce strict data residency and interoperability standards through regulations like the Data Act.	Creates a viable, high-performance alternative to U.S. hyperscalers for handling sensitive data and mission-critical AI workloads.
Build an AI-Ready European Network	Invest in high-bandwidth, low-latency terrestrial and subsea cable infrastructure within Europe. Promote edge computing to reduce transatlantic data flows for real-time AI.	Reduces the performance penalty of using European clouds and ensures internal digital markets function smoothly without U.S. backbone links.

4.2 Pathways to AI Sovereignty

Using EU-based AI providers and running open-source LLMs on local hardware are the core solutions to achieving digital sovereignty for Europe. This approach offers clear benefits but also introduces significant, often complex, new challenges in exchange for the control it provides.

These two methods work together to reduce dependency on US-controlled AI infrastructure and data flows. **Mistral AI** (a French startup) is the most prominent European alternative, positioned as a "sovereign" option with its Apache-licensed models designed to run from the cloud to the edge. Open-source LLMs—including those from Meta, Google, or Mistral—allow for **complete local control** as they can be run on in-house European hardware, ensuring that sensitive data and critical operations never leave European jurisdiction.

Switching to this model exchanges one set of risks for another, which must be carefully managed.

Aspect	Benefits & Opportunities	Risks & New Dependencies
Legal & Regulatory Compliance	Offers a **structural advantage** for complying with the **EU AI Act**, GDPR, and EU data residency laws.	**Enforcement gaps exist**. Some providers, including European ones like **Mistral**, have not fully complied with the AI Act's transparency rules on training data.
Operational & Cost Control	**Predictable infrastructure costs** (not usage-based), **low-latency performance**, and **no risk of external API changes or outages**.	**High upfront cost** of GPU hardware, expertise, and energy. Requires significant **internal IT and MLOps resources** to deploy, maintain, and secure.

Aspect	Benefits & Opportunities	Risks & New Dependencies
Performance & Capability	**Full customisability** for specific tasks (fine-tuning) and control over updates and feature sets.	**Potential performance gap**: Top open-source models may **lag behind the frontier models** from OpenAI or Anthropic.
Supply Chain & Sovereignty	**Reduces strategic dependency** on US cloud providers for core AI logic and processing.	**Shifts dependency to hardware**: Europe is still critically dependent on **US-designed advanced chips (e.g., from NVIDIA)** for training and running these models.

Key implementation challenges and mitigations:

1. **Managing the Compliance Gap**: Even European providers may fall short of EU regulations. To manage this, you must **proactively demand transparency** (full training data disclosure, model cards) and have legal teams audit provider compliance.
2. **Building Internal Competence**: Success depends on in-house expertise. **Invest in specialised talent** for model operations, infrastructure security, and domain-specific fine-tuning.
3. **Creating a Sovereign Ecosystem**: A single company is not an ecosystem. You should support and integrate with other EU initiatives, such as:
    - **Alternative Infrastructure**: Explore the **GAIA-X** initiative for federated European cloud services.
    - **Policy & Guidance**: Utilise the **EU AI Act's regulatory sandboxes** for testing and guidance.
    - **Alternative AI**: Consider other European models like Aleph Alpha.

Strategic recommendations for European policymakers and businesses:

- **Dual Strategy is Essential**: Promote a hybrid model where **Mistral** and similar providers serve as the base layer for sensitive applications, whilst US providers may still be used for non-critical R&D.
- **"Open Weight" is Not "Open Source"**: Clearly differentiate between truly open-source projects and "open-weight" models like Meta's Llama. The latter often come with **complex licences** that can restrict commercial use. Favour models with permissive licences like Apache 2.0.
- **Sovereignty Starts at the Edge**: Prioritise **edge deployment** (e.g., using models like Mistral's Ministral 3) for latency, cost, and data control.
- **Regulation Must Be Enforced**: The **EU AI Act** is a powerful tool for sovereignty, but its transparency requirements must be **actively and uniformly enforced** against all providers, including European ones, to be effective.

This builds on 4.1's risks and links to Chapter 8's Chips Act for hardware sovereignty and Chapter 5's GAIA-X for cloud. For UK: Align with AI Safety Institute; Canada: Leverage CSE strategies.

4.3 Emerging Risks: Quantum Computing and Edge AI

Beyond core AI dependencies, emerging technologies like quantum computing and edge AI introduce additional geopolitical risks, amplifying vulnerabilities in the domains outlined in Chapter 3.

Quantum Computing Lags and Export Controls

Europe trails the U.S. and China in quantum hardware development, with only ~10% of global investment. Quantum systems could break current encryption (e.g., RSA) within years, exposing data in transit or at rest. U.S. export controls on quantum tech (under Wassenaar Arrangement) limit EU access to cryogenics and error-correction components, while China's quantum satellite (Micius) enables secure comms beyond EU reach.

- **Risks**: Post-quantum cryptography (PQC) migration lags; a "quantum winter" could freeze R&D if supply chains disrupt (ties to Ch3 semis).
- **Mitigation**: Accelerate EU Quantum Flagship (€1B+ funding); adopt NIST PQC standards by 2027. For UK/Canada: Integrate with Five Eyes quantum initiatives.

Edge AI for Sovereignty and Resilience

Edge AI—running models on local devices (e.g., smartphones, IoT)—reduces cloud dependency but requires sovereign hardware. In crises, edge deployment enables offline inference (e.g., Mistral models on EU chips), mitigating latency from disrupted networks (Ch3 telecom).

- **Risks**: Hardware shortages (NVIDIA edge GPUs export-controlled); energy demands strain grids (Ch3 energy).
- **Mitigation**: Invest in EU edge platforms (e.g., EPI processors); test hybrid cloud-edge for critical apps. Benefits: Lowers data flows, enhances privacy under GDPR.

These emerging risks underscore the need for proactive R&D, linking to Chapter 5's protocol sovereignty and Chapter 6's threats (e.g., quantum in cyber ops).

4.4 Conclusions

AI and emerging risks, from dual-use compliance to quantum threats, build directly on the foundational domains in Chapter 3, highlighting how these technologies amplify geopolitical vulnerabilities. Pathways like Mistral adoption and edge deployment offer sovereignty, but require integration with the internet core strategies in Chapter 5 to counter threats in Chapter 6. This chapter emphasizes the strategic imperative for European businesses to address AI as a core risk domain.

Chapter 5: Internet Core Sovereignty and Digital Resilience

This chapter delves into the foundational internet protocols like routing, name resolution, and secure communications, explaining how geopolitical tensions could disrupt them and what European businesses can do to build sovereignty. Executives will find high-level strategies for maintaining digital operations during crises, such as reconfiguring networks and adopting EU alternatives, with technical details on BGP, DNS, and PKI for deeper implementation. It connects to broader risks in Chapters 3 and 5, emphasising resilience in connectivity and trust.

5.1 Border Gateway Protocol (BGP)

> BGP is the core routing protocol that enables global internet connectivity by exchanging reachability information between autonomous networks, directing data traffic efficiently across borders.

If U.S.-based networks could no longer be trusted (due to espionage, sabotage, or geopolitical rupture), reconfiguring BGP for Europe would involve a multi-layered, continent-wide effort focused on **security, redundancy, and re-routed trust**. Here's what would need to be done:

1. Immediate Operational Security Measures

- **RPKI (Resource Public Key Infrastructure) Mandate:** Enforce universal RPKI adoption across European ASes (Autonomous Systems). This cryptographically validates that an AS is authorized to announce specific IP prefixes, preventing hijacks from untrusted U.S. networks.
- **BGP Filtering:** All European ISPs and IXPs would implement strict prefix and AS-path filtering:
  - Reject routes originating from or transiting exclusively through U.S. ASNs where possible.
  - Accept only known legitimate prefixes from European and other trusted regions.
- **BGP Monitoring & Anomaly Detection:** Deploy real-time monitoring (e.g., using tools like BGPStream, ARTEMIS) to detect and respond quickly to malicious announcements.

2. Architectural Reconfiguration: Creating a "Trusted Core"

- **European Internet "Moonshot":** Develop a **European Internet Exchange & Transit Backbone** with minimal dependency on U.S. transit.
  - Incentivize major European Tier 1/2 providers (e.g., Deutsche Telekom, Orange, Telecom Italia, Telia) to peer extensively within Europe.
  - Expand capacity at major IXPs (AMS-IX, DE-CIX, LINX, etc.) and create new regional IXPs in Southern and Eastern Europe to keep traffic local.
- **Trans-Atlantic Link Re-evaluation:**
  - Classify all trans-Atlantic cables as **"untrusted links."**
  - Install "policy gateways" at cable landing stations (in Europe) to scrub and filter all BGP updates from U.S. peers before they enter the European core.
  - Consider **encrypting all international transit** (via MACsec or IPsec) at the physical layer for cables still in use.

3. Geopolitical & Policy Coordination

- **EU-Wide Mandate:** The European Commission and ENISA (EU Agency for Cybersecurity) would likely issue a regulation (similar to NIS2) requiring:
  - A "Digital Schengen" for routing, ensuring intra-EU/EEA traffic stays within trusted geography.
  - Mandatory cooperation among European NRENs (National Research and Education Networks) like GÉANT to form a secure, high-capacity scientific and research network independent of U.S. paths.

- **New "Trusted Peering" Agreements:** Replace peering and transit agreements with U.S. giants (like Cogent, Lumen, AT&T) with:
  - Increased peering with alternative global hubs (e.g., in Asia, Latin America, Africa) for global connectivity.
  - Strengthened direct peering with neighboring regions (e.g., Med. cables to North Africa, terrestrial links to Turkey/Ukraine for Asia connectivity).

5. Technical Trust Overhaul

- **MANRS (Mutually Agreed Norms for Routing Security) Compliance:** Make MANRS requirements mandatory for all European ISPs.
- **BGPsec (if widely deployed):** Accelerate adoption of BGPsec, which provides path validation (not just origin validation like RPKI). However, BGPsec deployment is currently limited.
- **Internal Trust Anchors:** Potentially create a **European RPKI root** or a tightly controlled regional trust anchor, separate from the global RIR system (which is influenced by U.S.-based organizations like ARIN and the legacy IANA functions, though these are now under the global community).

5. Redundancy & Capacity Building

- **Submarine Cable Diversification:** Fast-track new submarine cables that bypass the U.S., e.g.:
  - Europe to Asia via the Middle East (or Russia, if politically possible).
  - Europe to Latin America via Africa or direct cables (e.g., EllaLink).
- **Satellite Internet as Backup:** Leverage European-backed satellite constellations (e.g., IRIS² – the EU's sovereign satellite initiative) for critical government and infrastructure backup links, reducing dependency on fiber. Note limitations: Satellites offer Gbps capacity vs. Tbps cables, higher latency (vs. 60ms), and jamming risks—use for low-bandwidth priority only (see Appendix F).

6. Contingency Planning for a "Splinternet" Scenario

- **Prefix De-aggregation Strategy:** In a crisis, European networks might need to announce more specific prefixes to attract traffic away from routes transiting the U.S., preventing blackholes.
- **Pre-configured "Break-Glass" Configurations:** Network operators would have pre-tested BGP configurations to:
  - Withdraw all routes learned from U.S. peers.
  - Prefer paths via Asia, Africa, or direct peering.
- **Critical Services Localization:** Ensure core Internet services (DNS root instances, major CDNs, cloud regions) have fully operational replicas within Europe, so traffic doesn't need to leave.

7. Long-Term Strategic Shifts

- **European Cloud & DNS Sovereignty:** Accelerate GAIA-X (European cloud initiative) and host more DNS root mirrors and TLD authoritative servers within Europe.
- **New Protocols Research:** Fund R&D into post-BGP architectures like **SCION** (which offers path-aware, trust-based routing) for critical infrastructure.

Major Challenges:

- **Economic Cost:** Increased transit costs within Europe and to other regions; potential slowdowns if alternative paths have higher latency.
- **Global Connectivity:** Isolating from U.S. networks could degrade performance to the Americas and potentially to parts of Asia that rely on U.S. transit.
- **Coordination Overhead:** Requires unprecedented cooperation between EU member states, regulators, and competing private operators.

Conclusion: Reconfiguring BGP for Europe in this scenario would be less about changing the BGP protocol itself and more about **enforcing strict security policies, reshaping physical and logical network topology, and shifting geopolitical alliances in the digital realm.** The goal would be to create a **resilient, trusted European routing sphere** that can operate autonomously if necessary, while maintaining selective, heavily guarded connectivity to the U.S. and the rest of the world. This would be a massive, multi-year undertaking akin to building a parallel, secured internet infrastructure.

5.2 Domain Name System (DNS)

> DNS is the internet's domain name resolution system, translating human-readable domain names (e.g., google.com) into IP addresses for routing traffic.

Bringing a new, European-controlled "root-level" DNS server online in a crisis is technically possible, but its practical effectiveness for maintaining a functional internet in Europe during a major outage is highly questionable. The core issue is that such a server would not be trusted by the global system or the devices within Europe.

 The Technical vs. Political Challenge

- **Technically Straightforward**: The basic software and hardware to run a root name server are not exotic. Many organizations globally run "instances" of the existing 13 root server identifiers . The EU could download the root zone file and set up a local copy .
- **Politically & Practically Insurmountable**: A new root server would have no authority within the global DNS hierarchy, which is governed by **ICANN and the 12 independent root server operators**. For it to be effective, every network, device, and DNS resolver in Europe would need to be reconfigured to use it, replacing the built-in list of the global 13 root server addresses. This is not feasible in a short-term crisis.

 How the Internet Would Actually Fail Without US connectivity, the problem isn't that European root server instances disappear. Several (like **I-Root in Sweden**, run by Netnod, and **K-Root in the Netherlands**, run by RIPE NCC) already exist physically in Europe . The real breakdown happens downstream in the DNS resolution chain:

1. **Root Servers (Physical OK, Logical Broken)**: European root instances could still answer queries. However, if they cannot connect to the master source for the root zone file (managed by **IANA/ICANN** based in the US) to get updates, they would be serving outdated information, unable to add new `.com` or `.org` websites .
2. **Critical Failure at TLD Servers**: This is the main point of failure. The servers that manage `.com`, `.net`, `.org`, etc., are largely operated by **US-based entities like Verisign**. Even if a European computer asks a European root server for `example.com`, the root server would respond with the IP address of the `.com` servers, which are likely hosted in the US and unreachable .
3. **Authoritative Name Servers**: Finally, the servers that hold the actual IP addresses for specific websites (e.g., your company's site) might also be hosted on US-based cloud platforms like AWS, making them unreachable.

 The More Realistic European Focus: DNS Resolvers Given the above, European digital sovereignty efforts are more focused on the **recursive DNS resolver** level. These are the servers your devices actually query. Here, there are active European projects:

Project / Service	Jurisdiction & Description	Role in a Crisis
DNS4EU	An EU-funded public DNS resolver service with servers **exclusively within EU member states**.	If TLDs were still reachable, this would keep queries within European infrastructure, enhancing privacy and resilience
Quad9	A Swiss-based non-profit operating a global, secure DNS resolver	Provides a non-US jurisdiction alternative, though its global network might be affected by a US-EU split
National/Local Resolvers	Many European ISPs, organizations, and privacy groups run their own resolvers (e.g., in Germany, Austria, Luxembourg)	Local control at the resolver level is the most practical layer for sovereignty, though still dependent on the upstream TLD system

Recommendation for your planning: For true resilience in an extreme scenario, your organization should consider: 1. **Caching aggressively**: Configure internal DNS servers to hold records for critical domains for as long as possible. 2. **Maintaining a local hosts file**: For absolutely critical internal and partner services, maintain static IP-to-name mappings.

5.3 Certificate & Security Chain (HTTPS/TLS)

> HTTPS/TLS is the internet's secure communications protocol, using digital certificates to authenticate entities and encrypt data in transit, protecting against interception and tampering in contested environments.

If U.S.-based networks and services could no longer be trusted, the European digital certificate ecosystem would face immediate, systemic risks. The global HTTPS/TLS system relies overwhelmingly on U.S.-based **Certificate Authorities (CAs)** and the infrastructure they control. A rupture would compromise trust, validation, and encryption for nearly the entire web.

 The Central Risk: U.S.-Centric Trust Anchors The security of every `https://` connection ultimately depends on a list of trusted "Root Certificate Authorities" (Root CAs) hard-coded into your browser and operating system. These Root CAs are the ultimate issuers of trust. As of today: * **A majority of these globally trusted Root CAs are operated by U.S.-based companies** (e.g., DigiCert, Sectigo, Google Trust Services, Microsoft). * The technical and policy bodies that govern the rules for CAs—the **CA/Browser Forum**—are heavily influenced by U.S. corporate and legal frameworks.

In a crisis where U.S. entities are deemed untrustworthy, their Root CAs could be weaponized to: * **Issue fraudulent certificates** for European government, banking, or critical infrastructure sites, enabling perfect man-in-the-middle attacks. * **Revoke valid European certificates**, causing widespread outages for services that depend on them.

 A European Response Strategy To build a sovereign and resilient certificate chain, Europe would need to execute a multi-phase plan:

Phase 1: Immediate Mitigation & Aggressive Monitoring

- **Mandate Certificate Transparency (CT) Logs in EU Jurisdiction:** Require all certificates valid for EU domains to be logged in CT logs operated and controlled within the EU. This creates a public, auditable record to detect fraudulent issuance instantly.

- **Deploy Advanced Certificate Monitoring:** Implement tools like **Censys** or **Crt.sh** monitoring at a continental level to alert on any suspicious certificate issuance for critical `.eu`, `.fr`, `.de`, etc., domains, especially from non-EU CAs.
- **Promote EU-Based Public CAs:** Mandate the use of EU-headquartered CAs (like **GlobalSign** (BE/NL), **Sectigo** (though US-owned, has EU operations), or **D-Trust** (DE)) for all EU governmental and critical infrastructure services.

Phase 2: Building Sovereign Trust Infrastructure

- **Create a European Root CA:** Establish a new, **EU-government-backed Root Certificate Authority**. This is a political and technical project on par with creating a central bank.
- **Force-Injection into EU Devices:** Mandate through regulation (e.g., an expanded **Radio Equipment Directive**) that all devices sold in the EU must include this **"EU Trust Root"** in their trust store, alongside existing global roots.
- **Develop an EU-Only PKI Profile:** Define stricter technical and legal requirements for certificates used in Europe (e.g., mandatory hardware security modules, specific audit standards, data residency for validation services) that go beyond the global baseline.

Phase 3: Contingency Planning for Decoupling

- **Prepare for Mass Revocation:** Have technical and legal plans to **revoke trust in U.S.-based Root CAs** from European systems in a controlled, phased manner. This would be a "break-glass" action causing massive disruption but may be necessary.
- **Cross-Certification with Allied Trust Anchors:** Establish technical cross-certification agreements with other allied, non-U.S. root programs (e.g., in **Switzerland, the UK, Japan, or South Korea**) to create a broader "Allied Trust Network" as a counterbalance.
- **Accelerate Post-Quantum Cryptography (PQC):** Invest heavily in the adoption of **PQC algorithms** within the EU PKI. This future-proofs against a scenario where a hostile actor with a quantum computer could break current encryption and retroactively decrypt traffic.

 The Critical Link to BGP & DNS A sovereign security chain cannot exist in isolation; it must integrate with the reconfigured BGP and DNS layers: * **BGP + PKI:** If a European entity's IP space is hijacked via BGP, even a valid certificate is useless, as traffic can be redirected to an attacker's server. **RPKI (from the BGP section) is the essential companion to TLS certificates.** It proves ownership of the IP address, just as a certificate proves ownership of the domain name. * **DNS + PKI (DANE):** Europe could aggressively promote **DNS-Based Authentication of Named Entities (DANE)**. This technology uses DNSSEC (secured DNS) to store a website's TLS certificate or public key directly in its DNS record. This **bypasses the need for traditional CAs entirely**, anchoring trust in the DNSSEC chain, which Europe could control via its own root and TLDs (e.g., `.eu`).

 Major Challenges

- **Browser & Device Hegemony:** Major browser vendors (Google Chrome, Apple Safari, Microsoft Edge) and OS makers control the default trust stores. Gaining their acceptance for a new geopolitical root is a monumental challenge.
- **Global Interoperability Fracture:** If Europe uses a different set of trusted roots, European citizens and businesses may encounter "certificate warnings" when accessing non-EU websites, creating a fractured user experience.
- **Operational Complexity:** Running a Root CA at a continental scale with the requisite ultra-high security, availability, and legal liability is a massive, costly undertaking.

Conclusion Securing the certificate chain is about **controlling the source of digital trust**. Europe's path would involve: 1. **Monitoring** all certificate issuance for its domains. 2. **Building** its own sovereign root of trust and injecting it into the European digital ecosystem. 3. **Integrating** this trust layer with secured routing (RPKI) and DNS (DNSSEC/DANE) to create a defensible, end-to-end trusted internet infrastructure within its borders.

Without this, even with a secured BGP and DNS layer, the foundational trust behind every encrypted connection would remain vulnerable to external compromise.

Summary Table: Internet Core Protocols and Actions

Protocol	Key Risk	Mitigation	Reference
BGP (5.1)	Hijacking via U.S. routes	RPKI mandate, filtering, European backbone	MANRS compliance
DNS (5.2)	TLD unreachability	DNS4EU resolvers, aggressive caching	Quad9 alternatives
TLS/PKI (5.3)	U.S. CA weaponisation	EU Root CA, CT logs, DANE	Post-quantum migration

Building on AI and cloud risks from Chapters 3 and 4, this chapter provides the technical foundation for sovereignty. For deeper strategies on browsers, communications, and payments, see Appendix E (Cross-Cutting Toolkit).

5.4 Conclusions

This chapter's integrated approach—securing **BGP** routing with **RPKI**, **DNS** resolution via EU resolvers like **DNS4EU**, **TLS** trust through an EU Root CA and **DANE**—forms a defensible digital foundation. These measures directly counter the threat vectors in Chapter 6 (e.g., **DNS** hijacking in economic coercion) and inform the mitigation frameworks in Chapter 8 (e.g., continuity planning with Gaia-X). By implementing phased plans, European businesses can achieve operational autonomy in contested environments. Detailed browser/comms/payment strategies in Appendix E.

Chapter 6: Threat Vectors and Attack Scenarios

This chapter outlines the main ways adversaries could attack European technology infrastructure, from cyber operations and disinformation to physical sabotage and economic coercion, with real-world scenarios like grid blackouts or chip shortages. Executives can use these examples to assess potential business impacts and prepare response plans, while technical teams explore detailed tactics. It builds on previous chapters to highlight interconnected risks and the need for proactive defence.

Understanding the geopolitical context and critical technology domains is only the first step. To build resilience, European enterprises must anticipate *how* adversaries might exploit these vulnerabilities. This chapter outlines realistic, evidence-based threat vectors and plausible attack scenarios derived from current conflict patterns, intelligence reporting, and emerging hybrid warfare tactics.

6.1 State Sponsored Cyber Operations

Tactics & Actors

- **Russia**: **APT28** (Fancy Bear), **APT29** (Cozy Bear), and Sandworm continue targeting EU energy, transport, and government networks. Recent campaigns use **living off the land** techniques (e.g., abusing legitimate IT tools like PowerShell) to evade detection. In 2025, Sandworm was linked to intrusions into Polish rail systems, disrupting freight routes critical for EU supply chains.
- **China**: Groups like **APT41** (Winnti) focus on intellectual property theft in semiconductors, AI, and defence tech, often embedding malware in software supply chains. State backed acquisitions of European fabs (e.g., SMIC partnerships with German firms) enable long term espionage.
- **Iran & North Korea**: Increasingly active in ransomware and financial disruption, sometimes acting as proxies or opportunistic actors during wider crises. Iran's MuddyWater group has targeted European logistics firms, while North Korea's Lazarus has hit cryptocurrency exchanges.

Plausible Scenario: "GridLock Winter"

> In late November 2026, during a cold snap, Russian cyber units deploy a modified **Industroyer2 variant** against Polish and Romanian substations synchronized with Ukraine's grid. Simultaneously, disinformation floods social media claiming "EU energy rationing." Result: localized blackouts affect 2 million households, halting production lines in automotive factories reliant on stable power, and emergency cloud failover failures due to overloaded data centres. Economic losses exceed €500 million in the first week, with ripple effects on stock markets as insurers reassess cyber-physical risks.

6.2 Disinformation and Influence Campaigns Targeting Corporate Decision Making

Tactics & Goals

Adversaries increasingly weaponize information to:

- Undermine trust in EU regulatory frameworks (e.g., "NIS2 compliance is pointless" narratives);
- Sow division among corporate boards on sourcing decisions (e.g., "Huawei is safer than Ericsson");
- Manipulate stock prices or insurance premiums via false breach reports.

Plausible Scenario: "Chip Panic"

> Following ambiguous U.S. statements on Taiwan policy in early 2026, a coordinated bot network amplifies rumors that TSMC has halted all EU bound shipments due to geopolitical tensions. Automated trading algorithms trigger sell offs in automotive and industrial stocks, wiping €10 billion from European market caps in a single day. Procurement teams rush to prepay for "guaranteed" chip allocations from unvetted brokers, many of which are fronts for sanctioned entities, leading to supply chain compromises and regulatory fines under the EU Dual Use Regulation.

6.3 Physical Sabotage of Critical Infrastructure

Evidence from Current Conflicts

ACLED data confirms Russia's systematic targeting of Ukrainian energy infrastructure, with **~60 attacks per month in June and July 2025**, rebounding after a brief March moratorium. The **6 August 2025 strike on the Orlivka gas compression station**, directly on the Romanian border, demonstrates willingness to operate near NATO territory.

High Risk Targets in Europe:

- **Subsea cable landing stations** in Gotland (Sweden), Świnoujście (Poland), and Cuxhaven (Germany)
- **LNG terminals** in Wilhelmshaven and Krk
- **HVDC interconnectors** like NordLink (Norway–Germany) or LitPol Link (Lithuania–Poland)

Plausible Scenario: "Baltic Blackout"

> In early 2026, covert naval drones sever three major fiber optic cables in the Baltic Sea near Bornholm. Simultaneously, GPS spoofing disrupts maritime traffic, delaying repair ships by 48 hours. Financial transactions between Helsinki, Tallinn, and Stockholm halt for 72+ hours, costing €200 million in lost productivity. Cloud latency spikes force regional failover, but backup data centres lack sufficient power due to concurrent grid stress tests, exacerbating outages in ecommerce and remote work.

6.4 Economic Coercion via Sanctions, Counter Sanctions, and Market Access Restrictions

Emerging Dynamics:

- **U.S. policy shifts** (e.g., under Project 2025) could restrict American cloud or chip firms from serving certain EU sectors deemed "strategically sensitive."
- **China** may retaliate against EU EV tariffs by restricting exports of gallium, germanium, or graphite, critical for batteries and power electronics.
- **Russia** continues leveraging energy flows as political leverage, even post-pipeline.
- **U.S. NATO exit scenario**: A 6 month U.S. withdrawal from NATO could trigger tech sanctions on EU infrastructure, reciprocal EU restrictions, and rising sabotage risks like undersea cable tampering and DNS hijacking [New Scientist].

Plausible Scenario: "Transatlantic Tech Rift"

> In Q3 2026, the U.S. announces a 6 month NATO exit, imposing tech sanctions on EU critical infrastructure. U.S. cloud providers (AWS, Azure, GCP) terminate EU accounts via executive orders, while undersea cable sabotage disrupts internet connectivity and DNS hijacking redirects EU domains [Akamai]. Payment processing halts as the U.S. managed CHIPS network blocks EU transactions [U.S. Department of Homeland Security]. European businesses face operational paralysis, with many lacking EU only fallbacks for cloud, DNS, and payments [European Parliament]. DNS hijacking and cloud halts can be mitigated via Chapter 4's resolver caching (e.g., DNS4EU) and break-glass protocols (e.g., BGP filtering, EU Root CA for secure failover). Losses in the finance sector alone reach €1 billion daily, prompting emergency EU interventions like temporary data localization waivers.

Plausible Scenario: "Dual Use Dilemma"

> An EU medical device manufacturer integrates Chinese made AI vision chips into surgical robots. When the EU updates its Dual Use Regulation to include neural processing units, the company fails end user verification checks. Shipments are blocked at customs, triggering contract penalties and patient care delays, while competitors using legacy (non AI) systems

remain unaffected. The incident exposes supply chain vulnerabilities, leading to reputational damage and investigations under CSDDD for potential human rights risks in chip manufacturing.

6.5 Talent and R&D Espionage in Strategic Sectors

Vectors:

- Recruitment of researchers with access to quantum computing, advanced materials, or secure communications projects;
- Compromised open source libraries used in defence or energy software;
- "Academic collaboration" fronts masking intelligence collection.

Plausible Scenario: "Quantum Leak"

A European quantum encryption startup partners with a "neutral" Swiss research institute. Unbeknownst to them, the institute receives partial funding from a foreign state entity. Over 18 months, proprietary qubit stabilization data is exfiltrated, enabling an adversary to break current EU quantum safe cryptography standards years ahead of schedule. The breach is discovered during a routine audit, resulting in €50 million in lost contracts and accelerated adoption of compromised standards across EU defence networks.

6.6 Direct Military Interventions and Regime Changes

Emerging Dynamics:

- **U.S. unilateral actions**: As demonstrated by the January 2026 U.S. capture of Venezuelan President Nicolás Maduro, direct military interventions in geopolitically sensitive regions can disrupt global commodity flows, including oil and rare earths essential for European tech manufacturing.
- **Greenland acquisition efforts**: U.S. escalation in pursuing Greenland as a "national security priority" since late 2025, including threats of tariffs on EU trade, could fracture transatlantic alliances and impose economic coercion on European businesses.

Plausible Scenario: "Southern Hemisphere Shock"
> In February 2026, following the Maduro capture, U.S. forces intervene in another Latin American nation, seizing control of lithium mines critical for EV batteries. Global lithium prices spike 300%, halting European EV production and semiconductor fabs reliant on stable mineral supplies. EU sanctions against U.S. allies exacerbate the crisis, leading to retaliatory tech export bans and €2 billion in quarterly losses for European automotive and electronics sectors.

6.7 Conclusions

The threat vectors outlined—from cyber ops and disinformation to physical sabotage and economic coercion—illustrate the multifaceted risks to Europe's technology infrastructure. These scenarios, like "GridLock Winter" and "Transatlantic Tech Rift," highlight convergence and cascading effects, demanding the regulatory frameworks in Chapter 7 to bridge compliance gaps and enhance resilience.

1. **Convergence is the norm**: Cyber, physical, and informational attacks are rarely isolated. The most effective threats combine multiple vectors (e.g., cyber + disinfo + kinetic + economic coercion).
2. **Proximity matters**: Eastern and Central Europe face higher order risks due to geographic exposure, but no region is immune (e.g., subsea cables serve all of Western Europe; U.S. interventions affect global commodity chains).
3. **Second and third order effects dominate**: The primary target may be Ukraine, Taiwan, or Venezuela, but European businesses suffer collateral disruption through just in time supply chains, shared digital infrastructure, and transatlantic dependencies.

4. **Speed of escalation**: Geopolitical shocks can unfold in days (e.g., a Maduro style capture), requiring businesses to have preplanned responses rather than reactive measures.

Chapter 7: Regulatory and Compliance Landscape

This chapter reviews key EU regulations like the Cyber Resilience Act and NIS2 that govern technology risks, noting gaps in crisis scenarios and implications for transatlantic compliance. For executives, it highlights how to align business practices with these rules while building beyond mere compliance for resilience. It also covers export controls and due diligence, with notes on relevance for UK and Canadian contexts.

European enterprises operate within one of the world's most advanced regulatory ecosystems for digital technology and critical infrastructure. However, the intensifying geopolitical climate, marked by war in Ukraine, U.S. institutional volatility, and strategic competition with China, has exposed gaps between compliance and true resilience. This chapter outlines the key regulatory instruments shaping technology risk management and highlights where formal adherence may not suffice in crisis conditions.

7.1 EU Cyber Resilience Act (CRA) and NIS2 Directive

Cyber Resilience Act (CRA)

Adopted in 2023 and enforceable from 2025, the CRA imposes **lifecycle security obligations** on manufacturers of hardware and software with "digital elements." Key requirements include:

- Secure by design development practices
- Vulnerability disclosure timelines (≤15 days)
- Software bills of materials (**SBOM**s) for supply chain transparency

Implication: Companies sourcing firmware or embedded systems from non EU vendors (e.g., Chinese IoT device makers) must now verify CRA compliance or risk product recalls and liability for downstream breaches.

NIS2 Directive (Network and Information Security)

Effective October 2024, NIS2 significantly expands the scope of regulated entities to include:

- Medium sized energy, transport, health, and manufacturing firms
- Cloud infrastructure providers
- Public administration bodies

It mandates:

- Incident reporting within **24 hours** of detection
- Board level accountability for cybersecurity governance
- Regular stress testing against hybrid threat scenarios

Gap Alert: While NIS2 requires incident reporting, it does **not** mandate physical infrastructure redundancy (e.g., backup power for data centres during grid attacks) a critical omission given Russia's kinetic targeting of energy systems. NIS2 also enables mandates like those in Chapter 4's Digital Sovereignty Act for **RPKI** rollout and **DNS4EU** adoption.

7.2 GDPR in Conflict and Crisis Conditions

The General Data Protection Regulation remains foundational, but its assumptions are strained during active conflict:

- **Data breach reporting** (72 hour window) may be impossible if IT teams are displaced or systems destroyed.
- **Cross border data transfers** to U.S. cloud providers remain legally precarious under Schrems II, especially if a Project 2025 influenced U.S. administration weakens privacy safeguards or expands surveillance authorities.

- **Consent mechanisms** break down during mass displacement or emergency response, yet GDPR offers no explicit "wartime derogation."

Recommendation: Enterprises should preapprove **crisis mode data processing protocols** with national DPAs, including temporary use of encrypted satellite comms or sovereign cloud fallbacks.

7.3 Impact of U.S. Policy Shifts on Transatlantic Compliance

While the U.S. is not an EU regulator, its policies directly affect European operations through:

- **Cloud and software dependencies**: U.S. based SaaS platforms (e.g., Microsoft 365, Salesforce) may be compelled under the **CLOUD Act** to disclose EU customer data to U.S. authorities, even if stored in Frankfurt or Paris.
- **Export controls**: A Project 2025 aligned administration could restrict U.S. firms from providing patches, AI models, or chip design tools to EU entities deemed "strategically ambiguous."
- **Labor and vendor stability**: The OPM memo permitting federal employees to promote religious beliefs signals a broader reorientation of U.S. public-sector norms. While seemingly internal, such shifts can erode trust in U.S. regulatory consistency, especially for EU firms relying on American certified cybersecurity auditors or standards bodies (e.g., NIST).

Strategic Risk: Overreliance on U.S. validation ecosystems (e.g., FedRAMP, CMMC) may become a liability if transatlantic alignment fractures.

7.4 Export Controls on Advanced Computing and Dual Use Technologies

The **EU Dual Use Regulation (Regulation (EU) 2021/821)** now explicitly covers:

- AI systems capable of cyber intrusion
- Quantum sensors
- Advanced semiconductor manufacturing equipment
- Facial recognition and biometric surveillance tools

Businesses must conduct **end use due diligence** before exporting such items, even to allied countries, if there's risk of diversion to military or repressive uses.

Emerging Challenge: As China pressures third countries to adopt its surveillance tech, EU exporters face heightened scrutiny when selling to markets like Serbia, Kazakhstan, or the UAE. Failure to verify final use can result in:

- Fines up to **10% of global turnover**
- Debarment from public procurement
- Reputational damage under CSDDD (see below)

7.5 Due Diligence Requirements under the CSDDD

The **Corporate Sustainability Due Diligence Directive (CSDDD)**, effective 2027, requires large EU companies to:

- Identify actual or potential adverse human rights and environmental impacts in their **value chains**
- Prevent or mitigate those impacts
- Establish grievance mechanisms

While focused on sustainability, the CSDDD intersects with technology risk:

- A chip supplier using forced labor in Malaysia could trigger CSDDD liability
- A cloud provider sourcing colocation services from a firm with ties to Russian oligarchs may violate "adverse impact" clauses

Operational Note: CSDDD due diligence must now include **geopolitical risk mapping**, not just ESG metrics.

7.6 Gaps Between Compliance and Resilience

Despite this robust framework, several critical gaps persist:

Regulation	What It Covers	What It Misses
NIS2	Cyber incident reporting	Physical sabotage of cables or substations
CRA	Software security	Hardware tampering in transit
GDPR	Data privacy	Continuity during infrastructure collapse
Dual Use Reg.	Export screening	Inbound supply chain infiltration
CSDDD	Human rights	Strategic dependency on adversarial states

7.7 Conclusions

Compliance is necessary but insufficient. True resilience requires **going beyond checklists** to embed geopolitical scenario planning into governance, procurement, and architecture decisions, as amplified by collaboration in Chapter 9.

Chapter 8: Risk Mitigation Framework for European Businesses

This chapter offers practical strategies for mitigating technology risks through diversification, cyber defence, continuity planning, scenario exercises, and vendor management, tailored for European and allied enterprises. Executives can quickly identify key pillars to strengthen resilience, with actionable steps for implementation. It translates analysis from earlier chapters into business-focused frameworks for long-term stability.

Compliance alone cannot ensure continuity in an era of hybrid warfare, supply chain weaponisation, and transatlantic uncertainty. This chapter provides a proactive, multi-tiered mitigation framework that moves beyond regulatory checkboxes to operational resilience. It is structured around five pillars: **Diversification**, **Defence**, **Continuity**, **Scenario Planning**, and **Vendor Governance**.

8.1 Supply Chain Diversification & Onshoring Strategies

Strategic Goal: Reduce single points of failure in critical components and services.

Actions:

- **Map Tier 2 and Tier 3 suppliers** for semiconductors, optical transceivers, battery cells, and industrial control systems. Identify dependencies on Taiwan, China, or U.S. only vendors.
- **Qualify alternative sources** in trusted jurisdictions (e.g., Japan for memory chips, South Korea for displays, EU based PCB assemblers).
- **Accelerate participation in EU sovereign initiatives**:
  - Use **EuroHPC** for secure AI/ML workloads
  - Adopt **Gaia-X** aligned cloud providers for data residency
  - Partner with **European Processor Initiative (EPI)** for future CPU/GPU needs
- **Stockpile strategic buffers**: For mission critical hardware (e.g., **ICS** controllers, 5G radios), maintain 90–180 days of inventory, especially for components with >6 month lead times.

  Example: An automotive Tier 1 supplier shifts 30% of its MCU sourcing from TSMC to STMicroelectronics' new Crolles fab, accepting a modest performance trade off for guaranteed EU allocation.

8.2 Cyber Hygiene & Zero Trust Architecture

Strategic Goal: Assume breach; contain lateral movement.

Actions:

- **Implement Zero Trust Network Access (ZTNA)** for all remote and thirdparty connections, especially for OT environments.
- **Segment IT and OT networks** with unidirectional gateways (data diodes) where realtime control is required.
- **Enforce firmware integrity checks** using hardware rooted trust (e.g., TPM 2.0, Intel SGX) for servers and edge devices.
- **Adopt SBOMs (Software Bills of Materials)** and integrate them into vulnerability management platforms (e.g., automatically flag Log4j style risks).

  Critical Gap: Many European firms still allow corporate laptops to connect directly to factory floor networks. This must end.

8.3 Continuity Planning for Critical Infrastructure

Strategic Goal: Maintain operations during partial or total infrastructure loss.

Connectivity Resilience:

- **Diversify undersea cable paths**: Avoid reliance on single landing zones (e.g., don't route all traffic through Cuxhaven). Use satellite backup (e.g., Starlink Business, EU IRIS² constellation) for emergency comms.
- **Deploy mesh networking** at regional HQs to enable local coordination if internet fails.

Energy Autonomy:

- **Install microgrids** with solar + battery storage at data centres and manufacturing sites.
- **Pre negotiate emergency power agreements** with national grid operators for "critical enterprise" status.

Data & Compute Continuity:

- **Maintain sovereign cloud failover**: Replicate core workloads in at least two EU based regions (e.g., Azure Germany + OVHcloud France), aligning with Chapter 4's Gaia-X backbone and EU DNS resolvers for resilient routing.
- **Test offline operation**: Can your ERP run for 72 hours without cloud sync? If not, redesign. Incorporate Chapter 4's BGP filtering and DANE for secure, autonomous connectivity. See new subsection below for software licensing details.

  Reality Check: During the 2022 Ukraine blackouts, companies with local diesel generators and cached DNS survived; those dependent on cloud APIs did not.

Software Licensing Resilience Microsoft and other software dependencies create offline risks through activation and subscription checks. Audit licensing models to identify vulnerabilities.

Activation Type	Offline Behavior	Grace Period	Mitigation
MAK (Multiple Activation Key)	Works indefinitely after initial activation.	None after setup.	Use for air-gapped systems; pre-activate all devices.
KMS (Key Management Service)	Renews every 7 days; expires after 180 days without host contact.	180 days.	Maintain internal KMS host; plan secure check-ins or MAK fallback. Note: KMS host needs Microsoft contact every 180 days.
Subscription (e.g., M365)	Check-in every 30 days; reduced functionality after.	30-99 days.	Shift critical apps to perpetual licenses; test offline modes.
Perpetual Office (e.g., 2021)	Runs offline post-activation, but new setups need portal (no phone activation since Dec 2025).	Indefinite.	Stockpile install media; use VAMT for batch activation.

For SaaS (e.g., Adobe CC, Slack), expect full failure after grace periods—prioritise on-premises alternatives. Cross-ref Ch4.5 for comms (e.g., Matrix offline). For UK/Canadian firms, align with NCSC/CSE offline guidelines; inventory by model and test scenarios like "U.S. Cloud Freeze" (Ch5).

Software Category	Offline Impact	Examples
Subscription SaaS	Stops after 30 days; view-only mode.	Adobe CC, M365.

Software Category	Offline Impact	Examples
Perpetual	Full operation post-activation.	Office 2021, VLC.
Development Tools	Core offline; cloud features fail.	VS Code, Docker (local).

8.4 Geopolitical Scenario Planning

Strategic Goal: Stress test strategy against plausible, high-impact disruptions.

Conduct Tabletop Exercises for:

- **"Baltic Cable Cut"**: Simulate loss of 3+ subsea cables. Test financial transaction routing, employee comms, and customer support fallbacks.
- **"Taiwan Blockade"**: Model 60-day chip shortage. Identify which product lines can shift to older-node alternatives; which must halt.
- **"U.S. Cloud Freeze"**: Assume AWS/Azure/GCP restrict access to EU accounts due to U.S. executive order. Validate sovereign cloud migration playbooks.
- **"Hybrid Energy Attack"**: Combine cyber intrusion (grid SCADA) + drone strike (LNG terminal) + disinformation ("rolling blackouts"). Test crisis comms and board decision protocols.

Frequency: At least **biannual** for critical sectors; involve legal, procurement, and executive leadership, not just IT.

8.5 Vendor Risk Management

Strategic Goal: Ensure third parties do not become attack vectors or compliance liabilities.

Enhanced Due Diligence Measures:

- **Screen for ultimate beneficial ownership (UBO)**: Use tools like OpenSanctions or national business registers to detect hidden ties to sanctioned entities.
- **Require CRA and NIS2 compliance attestations** in all tech contracts, especially for cloud, SaaS, and embedded systems.
- **Embed continuity clauses**: Contracts should specify:
  - Minimum service levels during conflict
  - Right to audit physical security of data centres
  - Data portability guarantees within 30 days

Red Lines:

- No vendor with significant R&D or manufacturing in non EU jurisdictions should have **unrestricted remote access** to OT systems.
- Avoid sole source dependencies on vendors headquartered in countries with **extraterritorial data laws** conflicting with GDPR.

  Best Practice: A German energy firm now requires all ICS vendors to host maintenance portals within the EU and use certificate based authentication, not passwords.

8.6 Cross-Cutting Principles

1. **Resilience is a board level issue**: Technology risk must be reported alongside financial and operational risk.
2. **Sovereignty ≠ isolation**: Leverage global innovation, but anchor critical functions in trusted, auditable ecosystems.
3. **Test relentlessly**: A plan untested is a plan that fails.

8.7 Cross-Cutting Preparedness Toolkit

To operationalize the above mitigations across digital infrastructure:
1. Deploy a Gaia-X integrated dashboard [European Parliament] to monitor metrics in real time.
2. Conduct bi-annual supply chain audits via NIST SP 800-161r1 guidelines [NIST].
3. Mandate sector specific resilience plans (EU Digital Services Act amendment, 2026).
4. Stockpile EU made hardware for 6 month downtime scenarios.
5. Align workload placement strategies with Gartner's 2025 regional customer intimacy framework [Gartner] to reduce reliance on U.S. peering points.

8.8 Conclusions

The mitigation framework's pillars—diversification, defence, continuity, planning, and vendor governance—provide actionable steps to address risks from Chapters 2-6. By implementing these, European businesses can achieve resilience, amplified through the public/private collaboration in Chapter 9. This positions the continent to thrive in a contested landscape.

This framework equips European businesses not just to survive disruption, but to **maintain competitive advantage** when others falter. The next chapter explores how public/private collaboration can amplify these efforts at scale.

Chapter 9: Public/Private Collaboration and Policy Recommendations

This final chapter emphasises the importance of partnerships between governments, industry, and institutions to enhance technology resilience, with policy ideas like satellite funding and critical reserves. For executives, it outlines how to engage in coalitions and influence regulations for collective benefit. It concludes the book by linking collaboration to the mitigation strategies in Chapter 7.

No enterprise, regardless of size or sector, can achieve true technology resilience in isolation. The scale and complexity of today's geopolitical threats, ranging from undersea cable sabotage to semiconductor blockades, demand coordinated action across public institutions, private industry, and civil society. This chapter identifies high impact collaboration models and proposes actionable policy recommendations to strengthen Europe's collective technological sovereignty.

9.1 The Role of EU and National Institutions

ENISA (European Union Agency for Cybersecurity)

- **Expand threat intelligence sharing**: ENISA should operationalise a **classified but accessible feed** for NIS2 covered entities, modelled on the U.S. CISA AIS programme, but with **GDPR** compliant anonymisation.
- **Certify sovereign cloud and hardware**: Accelerate the **EU Cybersecurity Certification Framework** for cloud infrastructure, AI systems, and industrial control components.

EEAS (European External Action Service) & National Intelligence Agencies

- **Issue regular "Geopolitical Tech Risk Briefings"**: Quarterly updates for critical sectors on emerging threats (e.g., new Russian submersible capabilities, Chinese export controls on gallium).
- **Establish secure channels for private sector reporting**: Allow companies to confidentially report suspicious vendor behaviour or supply chain anomalies without triggering public disclosure requirements.

National CERTs/CSIRTs

- **Conduct joint cyber/physical war games**: Simulate coordinated attacks on energy grids + telecom backbones involving government responders and private operators.
- **Pre approve emergency protocols**: Define legal pathways for temporary data localisation, cross border incident response, and resource reallocation during crises.

9.2 Industry Coalitions and Information Sharing

Sectoral ISACs (Information Sharing and Analysis Centres)
Europe lags behind the U.S. in mature ISACs. Priority sectors should establish:

- **Energy ISAC EU**: For grid operators, LNG terminals, and hydrogen infrastructure
- **Tech ISAC EU**: Focused on semiconductor supply chains, cloud providers, open source software integrity, and internet core protocols (e.g., **BGP**/**DNS** experts per Chapter 4 for **RPKI** and **DNS4EU** coordination)
- **Finance ISAC EU**: To coordinate responses to payment system disruptions or SWIFT alternatives

These bodies should:

- Share **anonymised indicators of compromise (IOCs)** and **tactics, techniques, and procedures (TTPs)**
- Develop **common playbooks** for ransomware, cable cuts, and chip shortages
- Operate under **liability-safe harbours** to encourage transparency

Open Source Security Foundations
Given the ubiquity of open source software in critical systems, the EU should:

- Fund a **European Open Source Security Foundation** (modelled on OSS Fuzz) to audit high risk libraries used in **ICS**, cloud, and telecom
- Require **SBOM** submission for all public procurement software

9.3 Policy Recommendations for Strengthening Systemic Resilience

1. Fast-Track the IRIS² Satellite Constellation

The EU's secure broadband satellite network (IRIS²) must be prioritised for:

- Emergency communications during terrestrial outages
- Sovereign GPS alternatives to counter spoofing in Baltic/North Sea regions
- Secure data relay for remote industrial sites

Recommendation: Mandate that all NIS2 critical entities integrate IRIS² as a backup comms layer by 2028. Align with Chapter 4's Phase 4 for ICANN/IETF engagement on **DNS**/**PKI**.

2. Create a European Critical Technology Reserve

Modelled on strategic petroleum reserves, this would stockpile:

- Advanced node chips (for defence, health, and energy)
- Optical fibre spools and repeaters
- Industrial control system spares (RTUs, PLCs)

Funding: Jointly financed by member states and industry via a **Resilience Levy** on high risk tech imports.

3. Harmonise "Sovereign Cloud" Standards

Avoid fragmentation (e.g., Germany's Gaia-X vs. France's Cloud de Confiance). The EU should:

- Define a **common certification baseline** for data residency, encryption, and access control
- Incentivise adoption through **public procurement preferences**

4. Establish a Geopolitical Supply Chain Observatory

A centralised EU body to:

- Monitor real time disruptions (e.g., port closures in Taiwan, gas flow reductions)
- Publish risk scores for critical components (e.g., "TSMC 5nm: High Risk – 14-day buffer recommended")
- Alert businesses to emerging dual use export restrictions

9.4 Building a Culture of Collective Defence

Resilience cannot be outsourced to governments alone. Businesses must:

- **Share lessons learned** (even from near misses) via trusted industry forums
- **Participate in national crisis simulations**, not just observe
- **Invest in workforce readiness**: Train engineers in OT security, procurement teams in geopolitical risk assessment, and executives in crisis decision making

  Example: Following the 2023 Baltic cable incidents, Nordic telecom operators jointly funded a rapid response vessel stationed in Gotland, cutting repair time from 21 days to 5.

9.5 Conclusions: From Fragmentation to Strategic Cohesion

Europe's greatest vulnerability is not its dependence on foreign technology, it is the **fragmentation of its response**. By aligning regulation, investment, and information sharing around a common vision of digital sovereignty, European businesses can turn geopolitical adversity into a catalyst for innovation,

autonomy, and long term competitiveness. This collaborative approach culminates the frameworks in this assessment, equipping readers to lead in a resilient future.

Appendix A: Glossary of Geopolitical and Technical Terms

Term	Definition
APT (Advanced Persistent Threat)	State sponsored cyber actor conducting long term, stealthy operations (e.g., APT28 = Russian military intelligence)
Dual Use Technology	Items with both civilian and military applications (e.g., AI surveillance, quantum sensors), regulated under EU Regulation 2021/821
Hybrid Warfare	Combined use of conventional, cyber, economic, and informational tactics to destabilize adversaries without formal war
NIS2 Directive	EU law requiring enhanced cybersecurity measures and incident reporting for critical sectors
SBOM (Software Bill of Materials)	Inventory of open source and third party components in software, required under CRA
Zero Trust Architecture	Security model assuming no implicit trust; verifies every access request regardless of origin
Matrix Protocol	Open, federated messaging standard for sovereign communications (Ch4).
SaaS (Software as a Service)	Cloud-based subscription software vulnerable to connectivity loss (Ch7).
EU AI Act	EU regulation for high-risk AI transparency and compliance (Ch3).
LLM (Large Language Model)	AI systems for natural language processing, often reliant on U.S. models/hardware (Ch3).
Mistral AI	EU-based sovereign LLM provider with open-licensed models (Ch3).
Model Weights	Proprietary AI parameters under U.S. export control (Ch3).
OT (Operational Technology)	Hardware/software controlling physical devices (e.g., power grids, factory robots); distinct from IT
BGP (Border Gateway Protocol)	Internet routing protocol for exchanging reachability information between networks; vulnerable to hijacks in geopolitical ruptures (see Ch4).
Certificate Authority (CA)	Entity that issues digital certificates to verify the identity of websites and entities in TLS/PKI systems (Ch4).
Certificate Transparency (CT)	Public logging system for monitoring and auditing certificate issuance to detect mis-issuance (Ch4).
DANE (DNS-Based Authentication of Named Entities)	Protocol using DNSSEC to authenticate TLS certificates, bypassing traditional CAs for sovereignty (Ch4).
DNS (Domain Name System)	Internet's domain name resolution system, translating human-readable names to IP addresses (Ch4).
DNSSEC	Extension to DNS providing authentication of DNS data to prevent spoofing (Ch4).
MANRS (Mutually Agreed Norms for Routing Security)	Guidelines for improving BGP routing security through filtering and validation (Ch4).
PKI (Public Key Infrastructure)	Framework for managing digital certificates and public-key encryption (Ch4).
RPKI (Resource Public Key Infrastructure)	Cryptographic framework validating BGP route announcements to prevent hijacking (Ch4).

Term	Definition
SCION	Path-aware networking architecture for secure, policy-based routing as an alternative to BGP (Ch4).
Splinternet	Fragmentation of the global internet into regional silos due to geopolitical tensions (Ch4).
TLS (Transport Layer Security)	Protocol for secure internet communications, using certificates for authentication and encryption (Ch4).

Appendix B: Map of High Risk Infrastructure Corridors

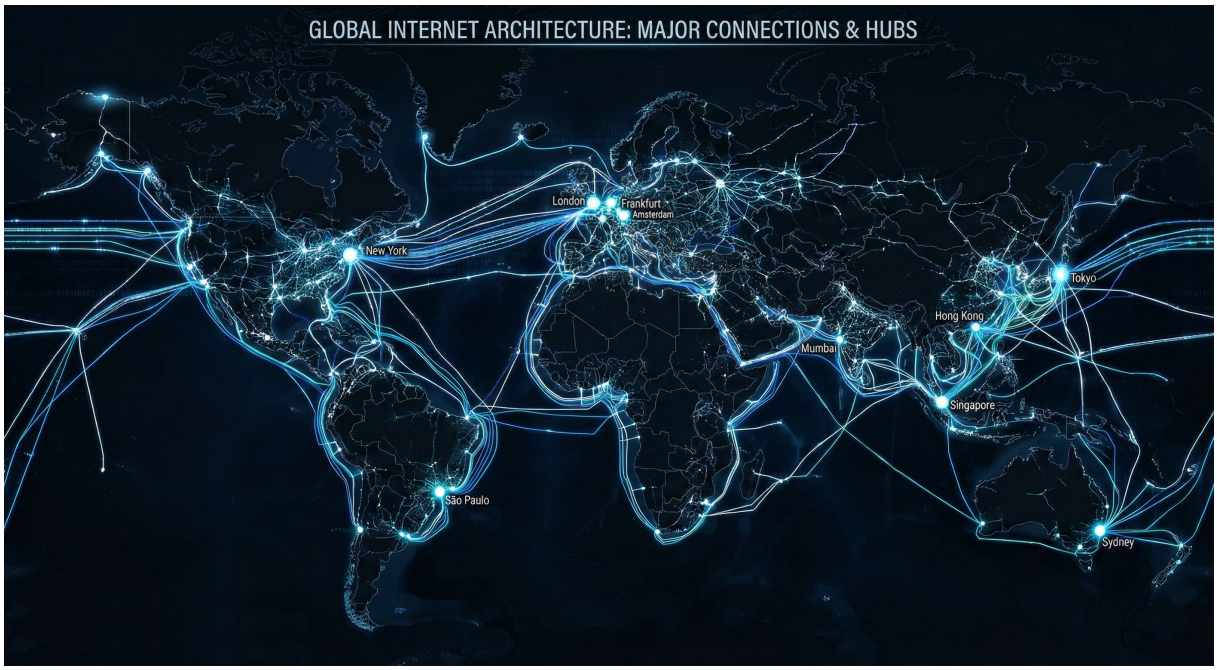

Figure 1: World Map of High-Risk Corridors

Undersea Cable Hotspots:

- **Baltic Sea**: Cables between Gotland (Sweden), Bornholm (Denmark), Tallinn (Estonia), and Klaipėda (Lithuania).
- **North Sea**: Routes linking UK, Netherlands, Germany (Wilhelmshaven/Cuxhaven), and Norway.
- **Black Sea**: Limited redundancy; vulnerable near Odesa and Constanța.

Energy Interconnectors at Risk:

- **LitPol Link** (Lithuania–Poland)
- **BRUA Pipeline** (Bulgaria–Romania–Hungary–Austria)
- **GIPL** (Gas Interconnector Poland–Lithuania)
- **Isaccea–Orlivka Power Line** (Romania–Ukraine border)

Semiconductor Supply Chokepoints:

- **Taiwan Strait**: >90% of advanced logic chips transit this zone
- **Strait of Malacca**: Critical sea lane for raw materials (e.g., neon gas, rare earths)

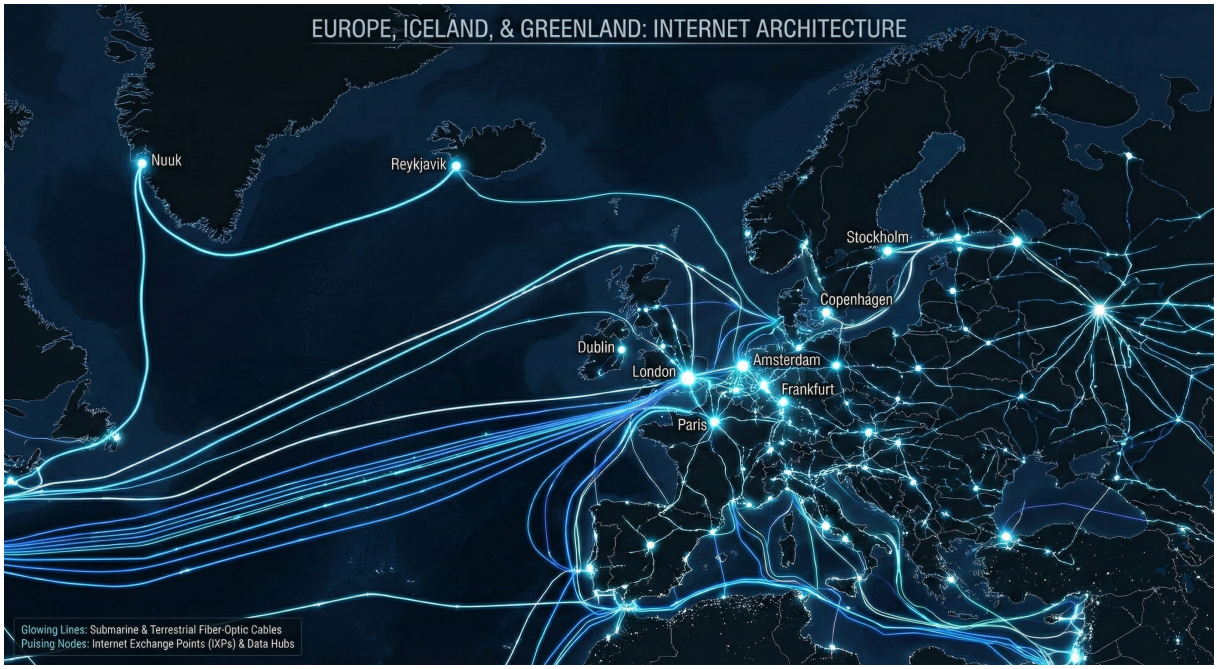

Figure 2: Detailed Europe Map of Infrastructure Risks

Appendix C: Technology Risk Self Assessment Checklist

Use this quarterly checklist to evaluate organizational readiness:

 Supply Chain

- Do we know the country of origin for all Tier 1 and Tier 2 hardware components?
- Have we identified at least one alternative supplier for critical semiconductors or cloud services?

 Cyber & OT Security

- Are IT and OT networks segmented with unidirectional data flow where possible?
- Do we maintain SBOMs for all custom and commercial software?

 Continuity Planning

- Can core business functions operate for 72 hours without internet or cloud access?
- Is emergency power available for critical systems (≥48 hours runtime)?

 Geopolitical Awareness

- Has leadership reviewed a “Taiwan blockade” or “Baltic cable cut” scenario in the past 12 months?
- Do procurement contracts include clauses for data portability and service continuity during sanctions?

 Internet Core Sovereignty (Ch4)

- Have we audited BGP peering dependencies and implemented RPKI validation?
- Is DNS resolution configured for EU resolvers (e.g., DNS4EU) with aggressive caching for critical domains?
- Do we have plans for TLS/PKI decoupling, including monitoring via CT logs and DANE adoption?
- For payments, have we tested EPI/wero fallbacks and Digital Euro integration?
- Browser/OS trust stores audited for EU Root CA compatibility (e.g., Firefox Sovereignty Build)?
- Comms sovereignty: Tested Matrix/EU-Connect for messaging; dual MX for email (Ch4.5)?
- Satellite backups: Planned for low-bandwidth priority (e.g., IRIS²; Ch3.1)?

 Software Licensing (Ch7)

- Audited Microsoft activation types (KMS/MAK grace periods)?
- Tested SaaS offline modes (e.g., 30-day M365 limit)?
- Inventory by license model; perpetual for critical apps?
- Procedures for offline activation (e.g., VAMT, portal jump box)?

Sample Data Residency Audit Checklist (from supplementary material):

1. Identify all sensitive data (financial, health, customer PII) stored on U.S. servers
2. Flag data subject to EU GDPR vs. U.S. CLOUD Act conflicts
3. Quantify downtime risk if U.S. authorities seize data

4. List EU based storage alternatives for high risk data

 AI Sovereignty (Ch3)
- Audited AI dependencies (hardware/models/cloud)?
- Tested Mistral/open-source LLMs for sovereignty?
- Enforced EU AI Act transparency for providers?

Appendix D: Key Resources

Conflict & Threat Monitoring

- ACLED Ukraine Conflict Monitor – Real time tracking of violence against infrastructure (https://acleddata.com/monitor/ukraine-conflict-monitor)
- ENISA Threat Landscape Reports – Annual cyber threat analysis (https://www.enisa.europa.eu/publications/threat-landscape)
- OpenSanctions – Database of sanctioned entities and politically exposed persons (https://www.opensanctions.org)

Regulatory Guidance

- EU Cyber Resilience Act (CRA) Text (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)
- NIS2 Directive Implementation Guidelines (https://ec.europa.eu/digital-single-market/en/network-and-information-security)
- EU Dual Use Regulation (2021/821) (https://trade.ec.europa.eu/doclib/docs/2021/may/tradoc_159631.pdf)

Sovereign Infrastructure Initiatives

- Gaia-X Association – European cloud/data infrastructure framework (https://gaia-x.eu)
- EU Chips Act Portal – Funding and project tracking (https://chips-act.ec.europa.eu)
- IRIS² Programme Overview – Secure EU satellite comms (https://digital-strategy.ec.europa.eu/en/policies/iris2)

Scenario Planning Tools

- ENISA's **CyCLONe** framework for cyber crisis coordination
- NATO CCDCOE's **CyCon** tabletop exercise templates
- World Economic Forum's **Global Cybersecurity Outlook** (includes private sector benchmarks)

Internet Core Tools (Ch5)

- RIPE NCC DNS4EU – EU sovereign DNS resolver (https://www.ripe.net/projects/dns4eu)
- ENISA PKI Guidelines – Public Key Infrastructure for sovereignty (https://www.enisa.europa.eu/topics/trust-services/pki)
- BGPStream – Real-time BGP monitoring tool (https://bgpstream.com)
- Censys Certificate Transparency – Monitoring for PKI risks (https://censys.io)
- ICANN Root Zone Management – Governance of DNS root servers (Ch5)
- IETF BGP Specifications – Standards for BGP and routing security (Ch5)
- Matrix.org – Open federated messaging for sovereign comms (Ch5.5; details in App E)
- Microsoft Activation Portal – Offline licensing guidance (Ch8)
- IETF MIMI WG – Messaging interoperability standards (Ch5.5; details in App E)

AI Sovereignty Tools (Ch3)

- Mistral AI – EU-based sovereign LLM provider (Ch3.6)
- EU AI Act – Regulation for high-risk AI (Ch3)
- Aleph Alpha – European AI foundation models (Ch3.6)

AI Sovereignty Tools (Ch3)

- Mistral AI – EU-based sovereign LLM provider (Ch3.6)
- EU AI Act – Regulation for high-risk AI (Ch3)
- Aleph Alpha – European AI foundation models (Ch3.6)

Additional Resources from Supplementary Material

- NATO HEIST (https://natoheist.org/)
- Interactive Internet map (https://map.kmcd.dev/?year=2025)
- Japan Times – Cloud market concentration analysis (https://japantimes.co.jp)
- Politico EU – Banking and tech dependency reports (https://politico.eu)
- Atlantic Council – U.S. authoritarian shift impacts (https://atlanticcouncil.org)
- European Council on Foreign Relations – Tech sovereignty plans (https://ecfr.eu
- New Scientist2464396-nato-tests-satellite-internet-as-backup-to-sabotaged-undersea-cables/) – NATO satellite backup for cables (https://www.newscientist.com/article/)2464396-nato-tests-satellite-internet-as-backup-to-sabotaged-undersea-cables/
- Akamai – DNS delivery and security (https://www.akamai.com/solutions/dns-delivery-and-security)
- European Parliament – EU cloud and data studies (https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778
- NIST – Supply chain risk management guidelines (https://csrc.nist.gov)
- Gartner – Infrastructure and operations insights (https://gartner.com)
- U.S. Department of Homeland Security – ICT supply chain reports (https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf)
- Merge.dev – API integration tools (https://merge.dev/blog/why-merge-is-more-extensible-than-you-think-a-guide-for-engineers)

Appendix E: Cross-Cutting Preparedness Toolkit

This appendix provides practical tools and detailed strategies for implementing sovereignty measures across chapters, including extracted content from Chapter 5 on browsers, communications, and payments. Use for technical teams to operationalize high-level recommendations.

Browser Sovereignty: Phased Strategy (from Ch5.4)

The case for a European sovereign browser remains strong, but it must be approached strategically.

1. **Ultimate Control Over the Trust Store:** A European browser (e.g., `EU Explorer` or `Aegis Browser`) would ship with the **EU Trust Root CA** pre-installed, allowing selective de-prioritisation of foreign roots. This decisively solves browser hegemony.
2. **Integrating Sovereign Tech Stack:** Native integration with EU projects, including default search to EU alternatives (e.g., Mojeek, Qwant), **DNS4EU**, **DANE** support, and **eIDAS 2.0** wallets. Privacy aligned with **GDPR** by default.
3. **Diplomatic and Standards Leverage:** A state-backed browser enhances negotiating power in the **CA/Browser Forum** and **W3C**, positioning Europe as a platform holder.
4. **Security from Ground Up:** Reduced attack surface with post-quantum cryptography and stripped legacy components.

Challenges

- **Cost & Complexity:** Multi-billion-euro effort for security patches, compatibility, and ecosystem building.
- **Distribution:** Regulatory mandates for pre-installation and user adoption against entrenched habits.
- **Fragmentation Risk:** Divergence could fracture the web, causing compatibility issues.

Phased Approach Phase 1: Leverage (Next 2-3 Years)

- **Regulate Trust Stores:** Mandate inclusion of **EU Trust Root** in all EU-distributed browsers via **Radio Equipment Directive** or **Digital Markets Act**.
- **Fund Firefox:** Invest hundreds of millions in Mozilla for an **"EU Sovereignty Build"** with default EU trust/privacy settings.

Phase 2: Hedge (Parallel, Long-Term)

- **Strategic Browser Reserve:** Fund a clean fork of Chromium/Gecko as a "break-glass" codebase for crises, synced with upstream fixes.

Phase 3: Moonshot (Decadal)

- **Trusted Client Initiative:** Develop a post-quantum client for government/critical sectors, expanding to public use.

Communications Sovereignty: Contingency for Email and Messaging (from Ch5.5)

European digital communication depends on US platforms, risking disruption in geopolitical ruptures.

Core Risks

- **Consumer Messaging:** Proprietary protocols (WhatsApp, iMessage) with US server control.
- **Enterprise Comms:** Cloud-tied tools (Teams, Slack) vulnerable to access revocation.
- **Email Backbone:** SMTP relies on US MTAs; DNS/PKI disruptions amplify failures.

Three-Pillar Plan Pillar 1: Activate Alternatives

- **Matrix as Standard:** Formalise Matrix protocol as **EUS-MSG-1**; launch **EU-Connect** app for government/critical use.
- **Sovereign Email:** Mandate EU cloud migration (e.g., GAIA-X); create `mail-relay.europa.eu` network.

Pillar 2: Break-Glass Comms

- **Crisis Packets:** Distribute USBs with Matrix clients and key caches.
- **Priority Layer:** Use EUROCONTROL/Galileo for low-bandwidth emergency messaging; develop Bluetooth mesh apps.
- **Email Decoupling:** Dual MX records with EU backups; trusted senders list via RPKI-like system.

Pillar 3: Long-Term Architecture

- **Project Dialogos:** Post-quantum, federated suite with **eIDAS** integration.
- **Protocol Diplomacy:** Standardise federation in IETF; fund EU contributions.
- **Sovereign Push:** Open-source alternative to Apple/Firebase.

Governance

- **ECR Regulation:** Suspend app exclusivity; prioritise sovereign traffic.
- **EDCA Authority:** Certify tools and run drills.

This integrates with Ch8.3 for offline continuity and counters Ch6 threats like "Transatlantic Tech Rift." For UK/Canada: Align with NCSC/CSE guidelines.

Payment System Sovereignty: Contingency Plan (from Ch5.4)

Current European payment infrastructure exists in a state of **strategic dependency** on US-controlled systems. In a rupture, disruptions to card networks (Visa/MasterCard), gateways (PayPal, Stripe), and settlement (SWIFT) could halt transactions.

Key Strategy: - Activate EPI/wero for instant payments; build standby engines with SEPA integration. - Develop Digital Euro rails for sovereignty; test cross-border fallbacks. - **Risk Metrics**: U.S. payment share >45% (target <20%); ensure 24-hour failover testing.

Implementation Steps: 1. Audit vendors for sanctions clauses. 2. Migrate 50% volume to EU rails (Adyen, wero) by 2027. 3. Stockpile offline POS hardware for retail.

Cross-ref Ch8 for vendor governance. Resources: EPI, Digital Euro.

AI Offline Note (Ch4)

Local LLMs via Mistral for inference; test edge deployment on EU hardware to ensure sovereignty during disruptions.

Appendix F: Offline Software Behaviors Guide

This appendix compiles behaviors of key software during extended offline periods, aiding continuity planning (Ch7.3). Focus on licensing and functionality impacts.

Microsoft Products Offline Summary

Product	Offline Behavior	Grace Period	Notes
Windows (MAK)	Indefinite after activation.	None.	Pre-activate; no phone option since Dec 2025—use portal on jump box.
Windows (KMS)	Expires after 180 days without host.	180 days.	Host needs Microsoft every 180 days; notification mode post-expiry.
M365 Apps	Reduced functionality (view/print only).	30-99 days.	Shift to perpetual for critical use.
Office Perpetual	Full after activation.	Indefinite.	Download media offline via connected device.
Exchange/SharePoint (On-Prem)	Full local operation.	None.	Internal network dependent; manual updates needed.

Non-Microsoft Desktop/SaaS Summary

Category	Offline Impact	Examples	Mitigation
Creative (Subscription)	Editing disabled after grace.	Adobe CC (30 days).	Perpetual alternatives; local assets.
Productivity SaaS	Core fails without cloud.	Google Workspace, Slack.	On-premises backups; test sync.
Dev Tools	Core offline; cloud features fail.	Docker local, VS Code.	Local registries; offline builds.
Comms	Real-time stops.	Teams, Zoom.	Matrix/EU-Connect (Ch4.5); mesh apps.

Satellite Connectivity Limitations (Ch3.1)

Issue	Impact	Mitigation
Capacity	Tbps cables vs. Gbps satellites.	Prioritise low-bandwidth (e.g., IRIS² for emergency).
Latency	60ms cables vs. higher satellite.	Non-real-time apps only.
Jamming	Easy disruption.	Layer with cables; electronic warfare drills.

Cross-ref Ch5.5 for comms, Ch8 for planning. For UK/Canada: NCSC/CSE equivalents.

AI Offline Note (from Ch4)

Local LLMs for offline inference; test edge deployment (e.g., Mistral models on EU hardware) to ensure sovereignty during network disruptions. Grace period: Indefinite post-setup; mitigate hardware dependencies via EU Chips Act stockpiles.